ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
Институт физики, технологии и экономики
Кафедра физики и математического моделирования

Создание цифрового контента для сопровождения информационной системы в организации

Выпускная квалификационная работа

Квалификационная работа
допущена к защите
Зав.кафедрой
д.ф.-м.н., профессор
Сидоров В.Е.

_____
подпись

Дата защиты:_

_____

Исполнитель:
студентка
Карагодина Ольга Петровна

_____
подпись

Научный руководитель:
к.п.н., доцент
Стихина Н.В.

_____
подпись

Екатеринбург, 2016

Оглавление

Введение

Процессы обмена информацией в мире, определяемые в значительной степени быстрым развитием информационных технологий, диктуют новые правила ведения деятельности предприятия и современные приемы к организации и управлению фирмой. Способы связи, преобразования и обработки информации достигли настолько высокого уровня, что управление отдельными предприятиями и целыми промышленными отраслями стало возможно с позиции управления единым организмом. Информационные системы предприятий становятся корпоративными информационными системами и гарантируют прозрачность ведения бизнеса предприятий. Существование разнообразных информационных систем позволяет своевременно реагировать на изменения внешних и внутренних условий, увеличивает рентабельность, делает предприятия привлекательными для размещения капитала с целью получения прибыли.

Современные компании требуют специалистов, уже обладающих знаниями в области обеспечения безопасности или самостоятельно обучают своих сотрудников. Необходимо обращать внимание на повышение осведомленности об актуальных угрозах, мерах и способах реализации атак и средствах защиты, фокусировать внимание сотрудников предприятий на важности обеспечения безопасности. Настоящий проект охватывает разработку, внедрение и эксплуатацию информационной системы в организации.

Современные специалисты информацию рассматривают как один из основных источников развития общества, а информационные системы и технологии как возможность повышения эффективности предприятия и деятельности сотрудников. Трудоспособность становится выше, если сотрудник умеет эффективно использовать информацию. Компетентный высококвалифицированный сотрудник финансового предприятия должен разбираться в получении, обработке и использовании информации с помощью персональных компьютеров, телекоммуникаций и других средств связи.

Когда необходимо обучить большое количество сотрудников без отрыва от работы и при отсутствии мотивации, а также не понести значительных финансовых потерь, тут может помочь только внедрение обучения сотрудников на основе электронных обучающих курсов корпоративной системы. Поэтому обучение сотрудников компании должно проходить дистанционно и содержать методы обязательного контроля. Непреднамеренные действия сотрудников финансового предприятия могут быть вызваны их незнанием или невнимательностью к правилам информационной безопасности, уклонением от выполнения требований и правил, принятых на предприятии. Важно пояснять сотрудникам, что выполнение правил по информационной безопасности это норма поведения, расширять их кругозор в области безопасности использования конфиденциальной информации, рассказывать на ежемесячной основе о существующих и новых техниках атак и методах защиты, что является основными задачами программы по повышению квалификации сотрудников финансового предприятия. Для классификации вышеуказанных задач понадобится создание в необходимом количестве образовательного цифрового контента.

Целью данного проекта является создание цифрового контента для сопровождения информационной системы в организации.

Для достижения поставленной цели были сформулированы следующие задачи:

- проанализировать возможные угрозы;
- предотвратить возможную реализацию угроз ИБ;
- повысить осведомленность сотрудников в области ИБ;
- увеличить степень ответственности сотрудников за свои действия.

Глава 1. Информация для обеспечения информационной безопасности финансового предприятия и создания цифрового контента.

Соблюдение правил по информационной безопасности - это направление в IT отделе организации, необходимое для защиты документов и массивов документов в информационных системах компании от неофициального доступа к ним как внутри компании, так и вне её. Информация - это ценные данные компании, которые нуждаются в надежных и своевременных мерах защиты.

Всё больше средств расходуется лидирующими компаниями различных областей рынка на развитие информационной безопасности. Так как несанкционированный доступ к информационным ресурсам влечет за собой огромные денежные и временные потери для организации.

Несанкционированный доступ в корпоративную сеть финансового предприятия может повлечь за собой следующие осложнения:

- стирание ценной информации, нарушение работы корпоративной сети. В результате компания несет затраты в связи с нарушением рабочего графика сотрудников;
- потеря информации. Попадание в чужие руки коммерческих секретов компании или информации о клиентах;
- мошенничество — запрещенное действие от лица вашей компании, например, с целью обогащения. Например, отправка электронной почты от имени служащих компании, внесение корректировок умышленного и неумышленного характера в текст страниц корпоративного веб-сайта или финансовых документов и т. п.

Как видно из приведенного определения целей защиты, безопасность информации — довольно обширная и многосторонняя проблема, охватывающая не только определение проблемы защиты информации, но и способы её защиты. Важным аспектом является не только создание политики информационной безопасности, но и обучающих электронных курсов для сотрудников финансовых предприятий. Электронный курс по информационной безопасности поможет научиться действовать в наиболее часто встречаемых ситуациях, когда важна осторожность в применении

информации. Большую часть инцидентов, связанных с информационной безопасностью, можно не допустить, поскольку около половины всех инцидентов порождают непосредственно сотрудники компании, так как не знают элементарных основ информационной безопасности. Соблюдение правил по информационной безопасности должно быть нормой поведения сотрудников финансового предприятия. Проанализировав большую часть инцидентов можно выделить шесть главных направлений, представленных на рисунке 1.

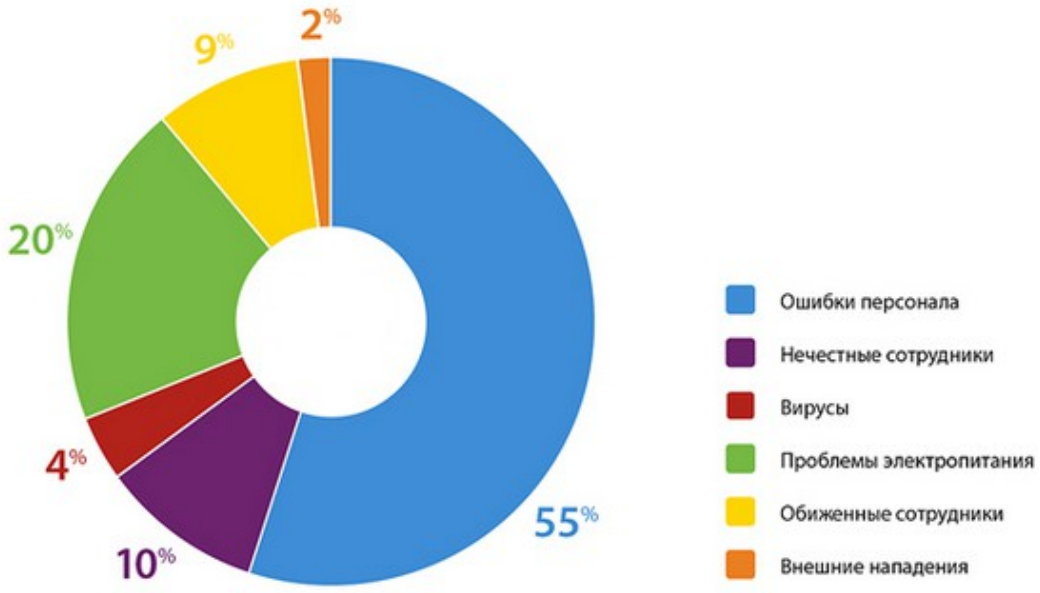


Рисунок 1 – Диаграмма инцидентов информационной безопасности

Когда необходимо обучить большое количество сотрудников без отрыва от работы и при отсутствии мотивации, а также не понести значительных финансовых потерь, тут может помочь только внедрение обучения сотрудников на основе электронных обучающих курсов корпоративной системы.

Сопровождение информационной системы в компании.

Информационная система является организационно–упорядоченная совокупность информационных ресурсов, информационных технологий, аппаратных и коммуникационных средств, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией.

ИС состоит из следующих основных компонентов:

1) программное обеспечение (ПО) – совокупность всей информации, данных и программ, которые обрабатываются компьютерными системами;

2) информационное обеспечение – обеспечение фактическими данными управленческих структур, использование информационных данных для автоматизированных систем управления, использование информации для обеспечения деятельности различных потребителей;

3) технические средства – комплекс электронных, электрических и механических устройств, входящих в состав системы или сети;

4) обслуживающий персонал.

Программное обеспечение представляет собой совокупность программ систем обработки информации и программных документов, необходимых для эксплуатации этих программ, и подразделяется на:

1) системное ПО – набор программ, которые управляют компонентами ИС, такими как процессор, коммуникационные и периферийные устройства, а также программы, предназначенные для обеспечения функционирования и работоспособности всей системы:

- операционные системы общего назначения, реального времени, сетевые, встраиваемые;
- загрузчик операционной системы;
- драйверы устройств;
- программы, способные выполнять преобразование потока данных или сигнала;
- утилиты;

2) программные средства защиты - программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты. К программным средствам защиты относятся:

- криптошлюзы;
- средства аутентификации;
- средства мониторинга и аудита;
- сканеры защищенности;
- средства разграничения доступа;
- системы криптографической защиты, шифрования и электронно–цифровой подписи;
- антивирусные и антиспамовые программы;

- межсетевые экраны;

3) инструментальное ПО – программы, предназначенные для использования в ходе проектирования, разработки и сопровождения ИС. Включает в себя средства разработки ПО, системы управления базами данных, компиляторы, трансляторы, генераторы;

4) Прикладное ПО включает:

- офисные приложения: текстовые редакторы, текстовые процессоры, табличные процессоры, редакторы презентаций;
- корпоративные ИС: бухгалтерские программы, системы MRP (Material Requirement Planning), системы MRP II, системы ERP (Enterprise Resource Planning System), системы CRM (Customer relationship management), системы SCM (Supply Chain Management), системы управления проектами, системы автоматизации документооборота, системы управления архивами документов, корпоративный портал;
- системы проектирования и производства: системы автоматизированного проектирования (CAD–системы Computer-Aided Design), CAE–системы (Computer-aided engineering), CAM–системы (Computer-aided manufacturing), PDM–системы (Product Data Management), PLM–системы (Product Lifecycle Management), автоматизированные системы управления технологическим процессом;
- системы логистической поддержки изделий: системы анализа логистической поддержки и организационно–технические системы;
- системы обработки и хранения медицинской информации;
- банковское ПО;
- геоинформационные системы;
- системы поддержки принятия решений;
- клиенты для доступа к интернет–сервисам: электронная почта, веб–ресурсы, мгновенная передача сообщений, чат–каналы, IP–телефония, P2P обмен файлами, потоковое вещание, клиент–банк;
- мультимедиа.

Платформа информационной системы содержит организационные и технологические подсистемы, комплекс обеспечивающих ресурсов, с помощью которых решаются как внутренние, так и внешние управленческие

и организационные задачи, в соответствии с функциями, определенными законодательством.

Информационная система обеспечивает взаимосвязанность подсистем в рамках единой логики, стандартов, «интерфейсов» и совместного использования информационных ресурсов.

К информационным ресурсам относятся:

1) базы данных и банк данных;
2) системная документация;
3) руководства пользователя;
4) учебные материалы;
5) операционные процедуры и процедуры поддержки;
6) планы обеспечения бесперебойной работы организации;
7) процедуры перехода на аварийный режим.

Технические средства используются для установки, поддержки и разъединения связи, а также для обеспечения преобразования сигналов между конечным оборудованием данных и каналом общего пользования, и включают:

1) компьютеры и логические устройства;
2) внешние устройства и диагностическую аппаратуру;
3) коммуникационное обеспечение;
4) энергетическое оборудование;
5) батареи;
6) аккумуляторы.

Коммуникационное обеспечение предназначено для управления процессами передачи информации между другими системами и включает в себя:

1) коммутаторы;
2) концентраторы;
3) маршрутизаторы;
4) межсетевые экраны;
5) адаптеры;
6) кабельные системы;
7) повторители, мосты.

Коммуникационное оборудование представляет собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и администрировать.

1.1 Общие положения политики информационной безопасности предприятия

Представленная ниже политика информационной безопасности предприятия позволяет создать общий подход в организации к защите информации, составляющей коммерческую тайну, устанавливает режим охраны конфиденциальных сведений от умышленного и неумышленного распространения или использования.

Положения политики распространяются на информацию, составляющую коммерческую тайну организации, независимо от вида носителя, на котором она хранится.

Информационная безопасность организации, заключается в обязательном соблюдении всеми филиалами организации правил и принципов, изложенных в политике информационной безопасности. Ответственность за соблюдение правил берут на себя сотрудники организации.

Информационная безопасность обеспечивается комплексной системой организационно-управленческих, административно-правовых, инженерно-технических и других мер защиты информации.

Перечень рисков информационной безопасности

Рисками информационной безопасности предприятия являются вероятные воздействия по отношению к информационным ресурсам, носителям сведений и технологическим ресурсам, связанным с обработкой и хранением сведений, составляющими коммерческую тайну финансового предприятия. Рост убытков финансовых предприятий обусловлен неправомерными действиями злоумышленников с целью хищения денежных средств со счетов клиентов банка или модификации внутренней информации. Проанализировав перечень рисков информационной безопасности, были выявлены следующие действия злоумышленников:

- несанкционированное изменение информации;
- повреждение (удаление) данных;

- неправомерный доступ к данным, образующим коммерческую тайну;
- распространение информации, то есть это преднамеренные или необдуманные действия с данными, составляющими коммерческую тайну;
- выход из строя техники, отвечающей за сохранение или преобразование данных, составляющих коммерческую тайну.

Модель действия нарушителя информационной безопасности

При построении модели нарушителя информационной безопасности используется неформальная модель злоумышленника (нарушителя), отражающая причины и мотивы действий, его возможности, априорные знания, преследуемые цели, основные пути достижения поставленных целей, способы реализации исходящих от него угроз, место и характер действия, возможная тактика.

По отношению к организации потенциальных нарушителей информационной безопасности условно можно разделить на внутренних и внешних.

К внутренним нарушителям относятся:

- сотрудники предприятия, имеющие полный или частичный доступ к конфиденциальной информации;
- технический персонал по обслуживанию предприятия.

К внешним нарушителям относятся:

- клиенты и посетители организации;
- сотрудники органов местного надзора;
- нарушители контрольно-пропускного режима;
- представители соперничающих предприятий.

Квалифицированность и техническая подготовленность вероятных нарушителей может быть самой различной от самого низкого навыка до специалистов уровня программистов.

Исходя из облика и вероятных вариантов действий внутренних нарушителей информационной безопасности можно перечислить такие действия как:

1) Действия сотрудников предприятия вне рабочего распорядка (пользователей персональных компьютеров). Это деятельность, которая может выражаться в нецелевом использовании ресурсов Интернет и электронной почты, самостоятельная установка и использование не разрешенного программного обеспечения. Подобные действия могут стать причиной распространения вредоносных программ, что может привести к потере данных на компьютерах и серверах организации, несанкционированному доступу злоумышленников к конфиденциальным данным.

2) Вход сотрудника компании во внутреннюю сеть с логином и паролем другого сотрудника может использоваться для выполнения нелегитимных действий во внутренней сети организации или краже конфиденциальной информации.

3) Установка на рабочую станцию, подключенную к внутренней сети организации, вредоносного программного обеспечения, позволяющего проводить исследование трафика сети и/или осуществлять атаки на ресурсы сети.

Исходя из неправомерного использования рабочих станций внутренними нарушителями можно перечислить следующие действия:

1) Неправомерное копирование конфиденциальных данных и информации.
2) Повреждение внутренней информации и данных клиентов на серверах и рабочих станциях предприятия.
3) Внесение неправомерных изменений в данные компании и программное обеспечение.
4) Похищение носителей с корпоративной информацией.
5) Похищение или вывод из строя техники, отвечающей за обработку и сохранение конфиденциальных данных.

Задачей внешних нарушителей информационной безопасности является нарушение бесперебойной работы сервисов удаленного доступа и публичных Интернет сервисов предприятия. Целью внешних нарушителей может являться один или несколько нижеперечисленных пунктов:

- захват управления Интернет сервисом предприятия;
- получение прав администратора информационной безопасности, доступ в корпоративную сеть организации;
- заражение компьютера сотрудника предприятия вирусом или другой вредоносной программой через сообщения электронной почты;
- неправомерное копирование конфиденциальных данных;
- стирание информации на серверах и компьютерах предприятия;
- неправомерные корректировки в данные и программное обеспечение предприятия;
- похищение носителей конфиденциальной информации;
- похищение или вывод из строя корпоративной техники, отвечающей за обработку и хранение конфиденциальных данных.

Исходя из всех выше перечисленных пунктов, можно сделать следующие выводы:

1)Неправомерный доступ к конфиденциальным данным и информации предприятия может быть следствием ошибок сотрудников предприятия, администраторов информационной безопасности, а также недостатков действующей технологии обрабатывания данных и т.д.

2) Определение возможных моделей нарушителей в значительной степени субъективно.

3) Как правило, особо подвержены мошенническим действиям: компьютеры, серверное оборудование, межсетевые мосты, коммуникационные каналы.

4) Сохранять в работоспособном состоянии составляющие автоматизированной системы важно от всех видов воздействий: стихийных бедствий и аварий, сбоев в подаче электроэнергии, отказов технического оборудования, ошибок сотрудников предприятия, ошибок в программном обеспечении и от преднамеренных воздействий злоумышленников.

5) Существует большой выбор вариантов преднамеренного или беспричинного неправомерного доступа к корпоративной информации, данным и нарушения работы процессов обработки и передачи внутренней информации.

6) Правильно построенная модель нарушителя, в которой отражаются его практические и теоретические возможности нарушить процесс обработки

и обмена информацией, активное мышление, время и место воздействия, а также иные характеристики - важная составляющая успешного проведения исследования риска и определения обязательных пунктов к составу и характеристикам системы защиты.

Требования к системе защиты информации финансового предприятия

Основным направлением информационной безопасности предприятия является своевременное выявление и управление информационными рисками, а также сведение их к минимуму.

Комплексная система защиты информации на предприятии базируется на следующих положениях:

- непрерывность во времени характеризует непрерывность проведения работ по защите информационной безопасности и реализацию комплекса мероприятий;
- комплексность определяет, что защита конфиденциальной информации должна быть всесторонней и предусматривать обеспечение физической целостности данных, предупреждение неправомерного изменения и предотвращение неправомерного получения и использования;
- целенаправленность, то есть это процесс, предполагающий принятие соответствующих действий на всех этапах жизненного цикла автоматизированной системы, начиная с ранних стадий проектирования;
- универсальность и надежность применимы для всех каналов проникновения и неправомерного доступа к автоматизированной системе предприятия и данных;
- плановость мероприятий по защите информации, предполагает опережение действий обеспечения безопасности информации, постановку задач по комплексной защите автоматизированной ситемы и реализацию мер обеспечения безопасности информации на ранних стадиях разработки автоматизированной ситемы;
- адекватность уровню важности защищаемых ресурсов предполагает соответствие уровня затрат предприятия на обеспечение сохранности информации, величине возможного ущерба от их распространения, утери, утечки, стирания или искажения исходных данных.

Все филиалы предприятия принимают участие в процессе защиты конфиденциальной информации, руководители филиалов должны держать на контроле данный вопрос.

Проанализировав способы защиты информации финансовых предприятий можно выделить следующие пункты:

1) личный допуск сотрудников организации к работе с конфиденциальной информацией и данными в пределах своих компетенций;
2) управление информацией и ресурсами для эффективного управления предприятием;
3) возможность идентификации и аутентификации работников предприятия;
4) ежедневное создание резервных копий важных информационных ресурсов предприятия;
5) ежедневное осуществление контроля целостности кода программного обеспечения от внешних и внутренних воздействий;
6) ежедневное проведение комплекса действий по борьбе с вирусами и другими вредоносными программами;
7) безопасное подключение корпоративной сети предприятия к сети Интернет;
8) возможность контроля над действиями сотрудников предприятия в корпоративной сети.

Объектами информационной защиты являются носители конфиденциальных сведений, производственные процессы и оборудование, связанные с преобразованием данных.

К защищаемым объектам относятся:

- документы на бумажных носителях;
- съемные машинные носители информации, на которых в электронном виде хранятся конфиденциальные сведения;
- компьютеры и сервера организации;
- сетевая техника;
- программно-аппаратные средства защиты информации;
- коммутационные каналы.

При рассмотрении угроз информационной безопасности объекта особое внимание необходимо уделить классификации подлежащих защите

объектов информационной безопасности финансового предприятия. Таким образом, можно сделать вывод о том, что действие угроз информационной безопасности объекта направлено на создание возможных каналов утечки защищаемой информации (предпосылок к распространению конфиденциальной информации за пределами организации) и само распространение конфиденциальной информации. Одно из ключевых понятий в оценке эффективности проявления угроз объекту информационной безопасности — ущерб, наносимый этому предприятию в результате воздействия угроз.

В любой финансовой компании определены объекты контроля, правила их перемещения и изменения, расписаны роли пользователей и определены наказания за нарушения. Также руководство по информационной безопасности понимает, что необходимо обучить персонал правилам обращения информации в компании. Ведь без постоянной работы с сотрудниками по поддержанию и совершенствованию процессов компании ни одно средство защиты не стоит потраченных на него денег. Руководители организации и филиалов принимают правила обращения информации в компании, признают систему контроля этих правил и ответственность за их нарушение, соблюдают правила работы с конфиденциальной информацией (являясь примером для своих сотрудников). Любые факты нарушения правил ИБ будут вскрыты и нарушители понесут ответственность за свои действия.

Руководители филиалов предприятия несут персональную ответственность за соблюдение режима информационной безопасности сотрудниками своих подразделений. Сотрудник несет ответственность за разглашение коммерческой тайны во время работы на предприятии и в течение двух лет после увольнения.

Разглашение сведений ограниченного распространения и нарушение режима информационной безопасности является чрезвычайным происшествием. По всем фактам проводится служебное расследование комиссией, назначаемой приказом директора предприятия.

Доступ сотрудников финансового предприятия к сведениям, составляющим коммерческую тайну

Допуск сотрудников предприятия к сведениям ограниченного доступа должен осуществляться в соответствии с их должностными инструкциями, в пределах необходимых для выполнения служебных обязанностей.

Выделение прав и полномочий сотрудникам предприятия для работы со сведениями ограниченного доступа в системах электронного документооборота предприятия производят администраторы автоматизированных систем.

Сотрудники, допущенные к работе со сведениями ограниченного доступа, должны выполнять все ниже перечисленные пункты:

- быть ознакомленными и выполнять все требования в области информационной безопасности и других инструкций, принятых руководством предприятия по информационной безопасности;
- немедленно сообщать своему непосредственному начальнику о вероятных причинах или фактах утечки конфиденциальной информации на предприятии;
- изучать конфиденциальные сведения только в объемах своих служебных обязанностей и не более;
- сразу сообщать руководству об утере, искажении носителей конфиденциальных сведений;
- сразу сообщать руководству и начальнику службы безопасности предприятия о всех попытках посторонних лиц получить доступ к конфиденциальным данным.

Проведя анализ, существующих угроз информационной безопасности можно сделать вывод о том что, сотрудникам предприятия, допущенным к работе с конфиденциальными данными, нельзя:

- использовать конфиденциальные сведения в открытой переписке, социальных сетях, публичных выступлениях;
- использовать конфиденциальные данные в собственных целях;
- вести обсуждение вопросов безопасности конфиденциального характера в общественных местах без разрешения пресс-службы и службы безопасности;

- выносить с охраняемой территории предприятия носители конфиденциальных сведений без согласования с непосредственным руководством.

Правила размещения элементов компьютерной сети

Под элементами компьютерной сети следует понимать следующее оборудование:

- съемные машинные носители, на которых производится запись конфиденциальных данных;
- рабочие станции и сервера организации;
- сетевое оборудование (маршрутизаторы, коммутаторы);
- программно-аппаратные средства защиты информации (межсетевые экраны, средства шифрования).

Условия размещения элементов компьютерной сети финансового предприятия должны обеспечивать:

- сохранность элементов компьютерной сети;
- исключение возможности неправомерного доступа посторонних лиц.

Обеспечение режима информационной безопасности при работе с ресурсами Интернет и электронной почтой

Развитие Интернет-технологий повлекло за собой появление и значительное распространение новых видов угроз по информационной безопасности, а также механизмов их реализации. Действующие в финансовых предприятиях системы антивирусной и антиспам защиты пришли в негодность, стала очевидной необходимость их усовершенствования. Применяемые решения выявили необходимость переосмысливания технологического подхода к обеспечению безопасной работы сотрудников предприятия с Web-ресурсами. Важно повысить гибкость управления политиками информационной безопасности, а также обеспечить контроль использования ресурсов Интернет в объеме всех подразделений финансового предприятия.

Присоединение корпоративной сети предприятия к сети Интернет должно осуществляться через межсетевой экран. Весь входящий и исходящий трафик предприятия должен проходить через фильтры межсетевого экрана. Межсетевой экран управляется локально или удаленно с определенного IP-адреса администратора. В настройках межсетевого экрана должны быть закрыты все не используемые сервисы и протоколы, корректность установленных свойств необходимо проверять руководством по информационной безопасности. Необходимо постоянно обновлять программное обеспечение межсетевого экрана, устанавливать все необходимые для работы дополнения. Серверы с размещенными на них Интернет-сервисами должны размещаться в демилитаризованной зоне, созданной межсетевым экраном. Данное условие выполняется при разделении локальной сети и публичных серверов на отдельные части. Та, в которой будут размещены публичные сервисы, как раз называется "демилитаризованной зоной".

Доступ к FTP должен быть разрешен только изнутри наружу и определенному списку внутренних пользователей предприятия. При необходимости доступа снаружи внутрь необходимо использовать усиленную аутентификацию.

Доступ сотрудников предприятия к сети Интернет должен осуществляться только через прокси-сервер предприятия. Межсетевой экран и прокси-сервер должны вести детальные системные журналы всех сеансов. Доступ к журналам должны иметь ограниченное число сотрудников предприятия, в основном для просмотра. На межсетевом экране и/или прокси-сервере должны вестись "Стоп-листы" ресурсов Интернет сомнительного содержания.

Межсетевой экран или прокси-сервер должен разрешать загрузку только тех программ на ActiveX, Java, Javascript, которые разрешены. Настройки межсетевого экрана или прокси-сервера должны запрещать загрузку программного обеспечения, кроме ограниченного круга пользователей.

Операционные системы и программное обеспечение Интернет-серверов предприятия должны содержать все исправления, рекомендованные производителем.

Интернет-серверы предприятия, работающие под UNIX-подобными операционными системами, не должны запускаться с правами суперпользователя.

Безопасность WWW-сервера предприятия.

Все общедоступные WWW-сервера предприятия, подключенные к Интернету, должны находиться в демилитаризованной зоне либо вне зоны корпоративной сети. Сведения ограниченного распространения не должны размещаться на публичном WWW-сервере предприятия.

Перед публикацией на WWW-сервере предприятия информация, должна быть просмотрена и утверждена так же, как утверждаются официальные документы предприятия.

Все публично доступные WWW-сервера предприятия должны регулярно тестироваться на предмет корректности ссылок.

Доступ пользователей в сеть Интернет.

Веб-браузеры должны быть сконфигурированы так, чтобы выполнялись следующие правила:

- доступ в Интернет должен осуществляться только через прокси-сервер предприятия;
- каждый загружаемый файл должен проверяться на вирусы и троянские программы;
- пользователям без особого разрешения запрещается устанавливать и использовать внешние почтовые сервера и внешние прокси-сервера.

Использование корпоративной электронной почты.

Электронные файлы, содержащие конфиденциальные данные, не должны отправляться с помощью электронной почты, а именно по открытым каналам в незашифрованном виде.

Сотрудниками могут использоваться только разрешенные администратором сети почтовые программы, заранее предустановленные.

Никто из посетителей предприятия или временных сотрудников не должен пользоваться электронной почтой предприятия без допуска.

Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не домену предприятия.

Связь с территориально удаленными подразделениями предприятия должна осуществляться только по закрытым каналам связи с использованием средств криптографической защиты информации.

Контроль выполнения мероприятий по информационной безопасности при работе в сети Интернет и использованию электронной почты возлагается на администратора компьютерной сети при содействии руководства.

Ведь если не соблюдать данные правила по информационной безопасности, то речь может зайти об утечках неких внутренних файлов (бизнес-планов, финансовых отчетов, технологической документации и т. д.). Когда информация об утечке всплывет в результате распространения данных в сети Интернет или в более неблагоприятном случае из-за какого-либо инцидента, связанного с незаконным использованием утекших данных, сделать что-либо уже будет невозможно.

Обеспечение режима информационной безопасности на рабочих станциях

На всех компьютерах сотрудников должен соблюдаться антивирусный контроль с автоматическим обновлением антивирусных баз.

Использование на компьютерах дисковых ресурсов с общим доступом должно допускаться только в привилегированных случаях, по заранее оформленному допуску.

Использование на компьютерах накопителей со съемными машинными носителями информации и портов USB должно допускаться в привилегированных случаях, по заранее оформленному допуску.

Компьютеры, на жестких дисках, которых хранится конфиденциальные данные, должны защищаться программно-аппаратными комплексами защиты информации от неправомерного доступа с возможностью криптографической защиты хранящейся базы с данными.

Сотрудникам финансового предприятия необходимо запретить:

- входить в компьютерную сеть предприятия, используя чужой логин и пароль;

- оставлять без присмотра не заблокированный монитор компьютера;
- самостоятельно изменять аппаратную или программную конфигурацию компьютера;
- самостоятельно устанавливать на компьютер программное обеспечение;
- разрешать другим лицам работу на компьютере со своими правами доступа;
- запрещается загружать из сети Интернет программное обеспечение;
- запрещается отключать антивирусное программное обеспечение, установленное на компьютере, и изменять его настройки.

Пользователь компьютерной сети предприятия должен:

- соблюдать требования регламентирующих документов по информационной безопасности;
- использовать персональный компьютер и ресурсы компьютерной сети предприятия только для выполнения своих прямых служебных обязанностей;
- сохранять рабочие материалы и документы в электронном виде в специально выделенном каталоге файлового сервера;
- блокировать монитор компьютера при потребности покинуть рабочее место, даже при кратковременном отсутствии;
- выключать рабочую станцию при уходе с рабочего места.

Контроль над действиями пользователей компьютерной сети осуществляется по протоколам, формируемыми информационными системами администратором компьютерной сети. Объем контрольных мероприятий и их периодичность указывается в должностных обязанностях соответствующих специалистов и в контрольных функциях соответствующих подразделениях финансового предприятия.

Применение парольной защиты

Прежде чем приступить к перечислению необходимых требований, которые следует предъявлять к паролям, используемым сотрудниками предприятия в корпоративной сети, назовем документ, в котором данные

требования должны быть прописаны, — это парольная политика предприятия. Именно она должна быть частью комплексной политики предприятия в области информационной безопасности. В комплексной политике должны содержаться основные требования и положения, исходя из которых, впоследствии составляются должностные инструкции для сотрудников, прописываются пункты в трудовых договорах и т. д.

Информация о паролях пользователей является конфиденциальной информацией, предназначенной для идентификации и допуска каждого конкретного пользователя к выделенным ему информационным ресурсам.

Операционные системы рабочих станций, включенных в компьютерную сеть предприятия, должны иметь настройки, позволяющие исключить возможность просмотра вводимой парольной информации.

Операционные системы серверов должны быть настроены таким образом, чтобы исключить возможность ознакомления с парольной информацией любого из пользователей, включая Администратора.

Серверы должны быть защищены паролем на загрузку операционной системы и доступа к конфигурации BIOS.

Компьютеры рабочих станций должны быть защищены паролем на доступ к конфигурации BIOS. Компьютеры рабочих станций, на которых хранятся конфиденциальные сведения, должны быть защищены паролем на загрузку операционной системы.

Операционные системы рабочих станций должны быть настроены таким образом, чтобы блокировать паузы неактивности (хранитель экрана) с функцией парольной защиты. Время включения защиты не более 10 минут.

Операционные системы серверов должны блокировать вход в сеть после 3-х кратной ошибки в наборе пароля.

Настройка активного сетевого оборудования предприятия не должна давать возможности неправомерной переконфигурации, в связи, с чем каждое активное сетевое устройство должно быть защищено уникальным паролем администратора компьютерной сети.

При уходе сотрудника предприятия в отпуск системный администратор, на основании заявки руководителя подразделения предприятия, производит блокировку имени пользователя в информационной системе предприятия.

При увольнении сотрудника из предприятия, системный администратор, на основании обходного листа, производит удаление пользовательского имени в информационной системе предприятия.

Период действия паролей составляет 90 суток, после чего они подлежат замене на новые, ранее не применявшиеся.

Администраторам различных информационных систем запрещается использование административного пароля при повседневной деятельности, не связанной с административными функциями. Для этой цели Администраторам должен выделяться пароль с правами пользователя.

Пароли Администраторов и пароли BIOS серверов должны храниться в опечатанных конвертах в сейфе директора предприятия. Каждый пароль хранится в отдельном конверте.

Доступ в компьютерную сеть предприятия, через общедоступные каналы связи обеспечивается только с применением смарт-карт либо их полнофункциональных аналогов USB-брелков eToken.

Любые некорректные действия сотрудников, связанные с доступом в компьютерную сеть, рассматриваются как нарушения режима информационной безопасности и анализируются через процедуру служебного расследования.

Ответственным за настройку серверов и рабочих станций является администратор компьютерной сети.

Антивирусная безопасность

Под компьютерными вирусами, троянскими программами следует понимать программы, которые могут заражать другие программы, изменяя их посредством добавления своей, возможно модифицированной, копии, сохраняющей способность к дальнейшему размножению (далее по тексту вредоносные программы).

Возможными путями проникновения вредоносных программ в компьютерную сеть предприятия являются:

- сеть Интернет, путем загрузки пользователями зараженного программного обеспечения;
- загрузка WWW-страниц с активными приложениями, содержащими вредоносный код;

- заражение рабочих станций пользователей через электронную почту;
- распространение вредоносных программ через сеть Интернет и электронную почту посредством использования уязвимостей программного обеспечения;
- установка на рабочие станции и сервера предприятия зараженного программного обеспечения или электронных документов.

Возможные последствия распространения вредоносных программ в компьютерной сети предприятия:

- изменение, уничтожение данных;
- утрата информации из компьютерной сети предприятия;
- нарушение технологических процессов в компьютерной сети предприятия.

Выполнение всеми сотрудниками предприятия мероприятий, направленных на предотвращение проникновения вредоносных программ в компьютерную сеть предприятия, является основой нормального функционирования сети и одним из важнейших условий информационной безопасности.

Правила антивирусной защиты доводятся до всех пользователей компьютерной сети предприятия под личную роспись в журнале инструктажа администратором сети.

При передаче программного обеспечения и электронных документов в другие предприятия или физическим лицам необходимо проводить антивирусный контроль передаваемой информации.

Все факты проникновения вредоносных программ в компьютерную сеть предприятия являются нарушением информационной безопасности и подлежат служебному расследованию.

Контроль выполнения антивирусной безопасности пользователями компьютерной сети предприятия возлагается на информационно-технический отдел.

Резервное копирование

Резервное копирование является средством защиты информации, хранящейся в электронном виде, от повреждения либо уничтожения в результате сбоев программного обеспечения, сбоев и неисправностей вычислительной техники, а также в результате физического повреждения (уничтожения) вычислительной техники.

Объектами резервного копирования являются:

- базы данных автоматизированных информационных систем предприятия;
- программное обеспечение и данные, расположенные на файл-серверах;
- операционные системы серверов и настройки активного сетевого оборудования;
- критичное программное обеспечение и данные, расположенные на компьютерах пользователей.

Выводы

Обучение сотрудников предприятия - один из способов повышения рентабельности. Во многих крупных предприятиях обучение стало не только привычным, но и обязательным, выгода которую получает компания за счет повышения квалификации своих сотрудников существенна. Каждый день для сотрудников проходят различные профильные семинары, курсы, тренинги для бухгалтеров, программистов, менеджеров по продажам и т.д. Подобные мероприятия дают специализированные знания сотрудникам, чтобы они могли лучше выполнять свои профессиональные обязанности.

Также как и профильные курсы для сотрудников, курсы по обеспечению информационной безопасности для обычных пользователей имеют своей целью повысить эффективность функционирования компании. Однако такие курсы имеют свою специфику. Ниже рассмотрим, зачем нужны курсы по повышению уровня знаний в области информационной безопасности и какая форма обучения на предприятии наиболее эффективна.

По статистике больше половины потерь, которые несут компании из-за инцидентов в области информационной безопасности, вызваны действиями персонала. И в основном они происходят не из-за злого умысла, а просто из-

за низкого уровня осведомленности пользователей. Таким образом, обучая своих сотрудников основным правилам в области информационной безопасности, компания может значительно снизить риск нарушения информационной безопасности. Обучение персонала – одно из основных требований международного стандарта управления информационной безопасностью ISO/IEC 27001.

При выборе наиболее эффективной формы обучения можно столкнуться с большим количеством вопросов, которые на первый взгляд могут стать серьезной проблемой. Во-первых, нет возможности отправить одновременно на курсы по повышению квалификации сразу всех сотрудников предприятия – это не десять, не сто, часто даже не тысяча человек, и обучение потребует действительно очень больших финансовых вложений. Важно помнить, что во время обучения персонал отрывается от своих прямых обязанностей, что наносит компании весомый материальный ущерб. Пользователям мало просто один раз рассказать о правилах, которые необходимо выполнять для защиты информационных ресурсов компании. Обучение должно быть регулярным, что практически нереально, учитывая написанное выше. Деятельность компании просто остановится. И последняя основная проблема – отсутствие мотивации. Сотрудники чаще не заинтересованы в обучении, в основном относятся к нему негативно, так как рассматриваемые на курсах вопросы им непонятны, они усложняют их обычную работу, отрывают от привычного рабочего распорядка дня.. При таком отношении очень сложно достичь хороших результатов по повышению уровня защищенности информационных активов компании. Даже если действовать принудительно, трудно проконтролировать уровень знаний сотрудников на курсах, руководители предприятия и преподаватели не заинтересованы в уровне квалификации обучаемых и зачастую выдают сертификаты просто по факту прохождения обучающимся очередного курса.

Итак, если сравнить положительные и отрицательные стороны обучения сотрудников в области информационной безопасности, мало кто будет спорить, что минусов значительно больше. Надо понимать, что в

данном случае мы говорим только о внешних курсах, тренингах и семинарах. Внутренний очный инструктаж также необходимо проводить с сотрудником под роспись, при приеме на работу и через определенный промежуток времени. Но инструктаж и какие-то разовые мероприятия – одно, а организованное регулярное обучение – совсем другое. Всё больше компаний в последние несколько лет используют корпоративные системы повышения квалификации сотрудников финансового предприятия как наиболее оптимальный вариант обучения своих сотрудников. Причем, сразу надо оговориться, что речь идет не о дистанционном обучении через Интернет в различных учебных центрах, когда мотивация сотрудника должна быть еще выше, чем при очных курсах и семинарах, и при котором достичь необходимого уровня контроля над результатами труднее, чем на обычных курсах. Когда стоит задача обучить большое количество сотрудников без отрыва от работы при отсутствии мотивации у обучаемых, наладить эффективную систему контроля, сделать процесс регулярным, и при этом не понести значительных финансовых потерь, тут может помочь только внедрение корпоративной системы обучения сотрудников правилам информационной безопасности.

Проанализировав, ниже описано, что собой представляет корпоративная система повышения квалификации сотрудников финансового предприятия в наши дни. В первую очередь – это курсы и тесты, доступные любому количеству пользователей в любое удобное время. Простое управление графиком обучения, формирование любых групп обучающихся с назначением соответствующих курсов, тестов и сроков обучения, доступные в любое время отчеты по процессу обучения как каждого сотрудника, отдельных регионов, филиалов, отделов так и в целом всех сотрудников компании, то есть появляется возможность, по сути, получать метрики эффективности системы обучения для представления руководству. Кроме того, корпоративная система – это эффективная система контроля знаний с напоминаниями и уведомлениями, возможностью добавления любых курсов

и тестов, внутренняя система общения обучающихся с кураторами, причем, куратором может быть как сотрудник отдела информационной безопасности, так и специалист отдела кадров. Никаких специальных знаний, чтобы курировать процесс обучения сотрудников, не требуется. Благодаря всем этим возможностям легко достичь того, чего не дают обычные курсы – одновременное обучение большого количества сотрудников с небольшими затратами, причем если взять стоимость обучения одного сотрудника, то можно увидеть, что затраты получаются действительно минимальными. То же самое в отношении предприятия регулярных тренингов – практически без дополнительных вложений с любой регулярностью (обычно проводить обучение персонала рекомендуется дважды в год или раз в квартал) можно проводить очередной теоретический курс или практический тренинг с тестированием. При этом сотрудники знают финальную дату окончания каждого курса и сами могут планировать время обучения и прохождения тестирования, что позволяет свести к минимуму отвлечение от профессиональных обязанностей, которые все-таки всегда первичны.

1.2 Обзор электронных ресурсов для создания цифрового контента

Электронный контент — сведения, а также продукты и относящиеся к ним услуги, предоставляемые абонентам сетей передачи данных и сетей сотовой связи в электронном (цифровом) виде, потребляемые и используемые с применением устройств обработки цифровой информации.

Под «электронным информационным материалом» могут подразумеваться практически любые сведения, размещённые на электронном (цифровом) носителе информации: текст или же аудио-, видео-, фото файлы.

Рассмотрим ниже инструменты для создания электронных учебных материалов.

CourseLab – это внушительное и вместе с тем легкодоступное в эксплуатации средство для формирования интерактивных цифровых курсов, создаваемых для использования в сети Интернет или на съемных носителях, в системах удаленного или внутрикорпоративного обучения.

Благодаря CourseLab можно создавать и редактировать электронный курс в среде WYSIWYG, не обладая знаниями в области языков программирования.

Бесплатную англоязычную версию CourseLab можно скачать на официальном сайте. На русскоязычном ресурсе – ознакомится с прилагаемым проектным материалом или купить русскую версию продукта. Внешний вид ресурса представлен на рисунке 2.

Рисунок 2 – Сайт CourseLab

Рисунок 3 – Сайт Smart Builder

Smart Builder, представленный на рисунке 3 − это сервис, позволяющий создавать собственные электронные образовательные курсы, не обладая

навыками программирования или другими специальными знаниями. Существует возможность использовать различные медиа, игровые элементы и т.д. В библиотеке Smart Builder уже содержится множество элементов от мультимедиа объектов до шаблонов страниц. Возможности сервиса не ограничены, и готовый проект можно создать практически мгновенно в зависимости от изначальных условий. В значительной степени этому способствует удобный и интуитивно понятный интерфейс и многофункциональность, так как программный продукт состоит из нескольких модулей.

Рисунок 4 – Сайт Vyew

Vyew − это виртуальный конференц-зал или комната для переговоров. С помощью сервиса можно создать онлайн-презентацию перед сотней людей или опубликовать документ для совместного обсуждения и редактирования с коллегами. Внешний вид ресурса представлен на рисунке 4.

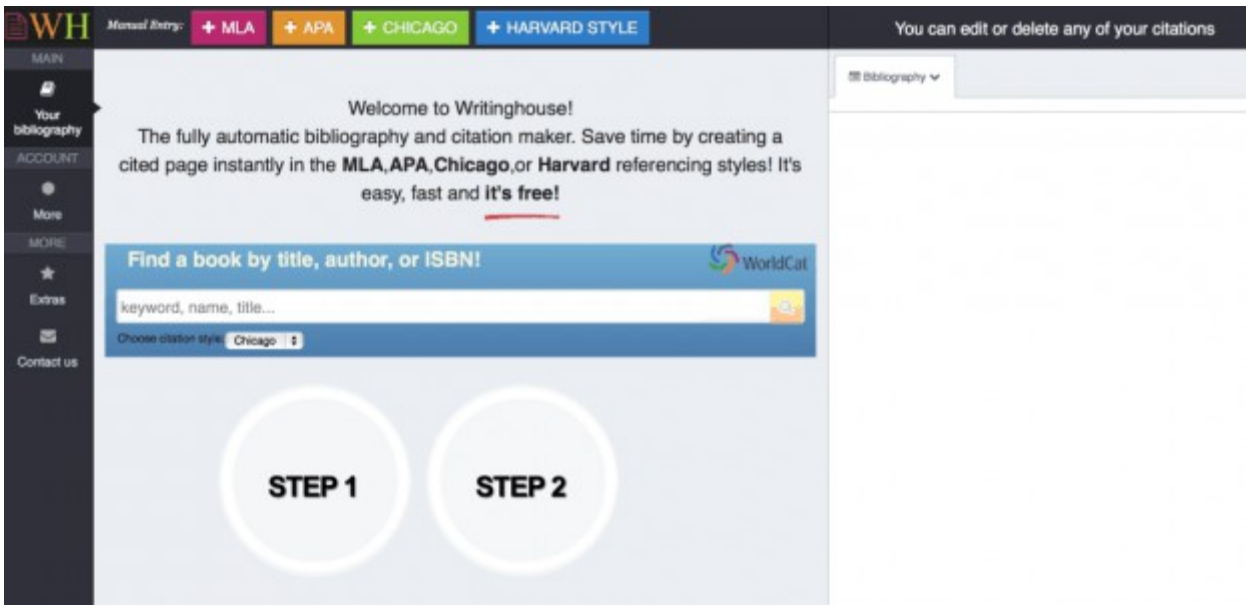


Рисунок 5 – Сайт Writing House

Writing House − это сервис, который позволит вам автоматически создавать библиографию и оформлять цитирование в основных стандартах − MLA, APA, Chicago или Harvard. Это быстро, просто, бесплатно и поможет вам сэкономить много времени. Внешний вид ресурса представлен на рисунке 5.

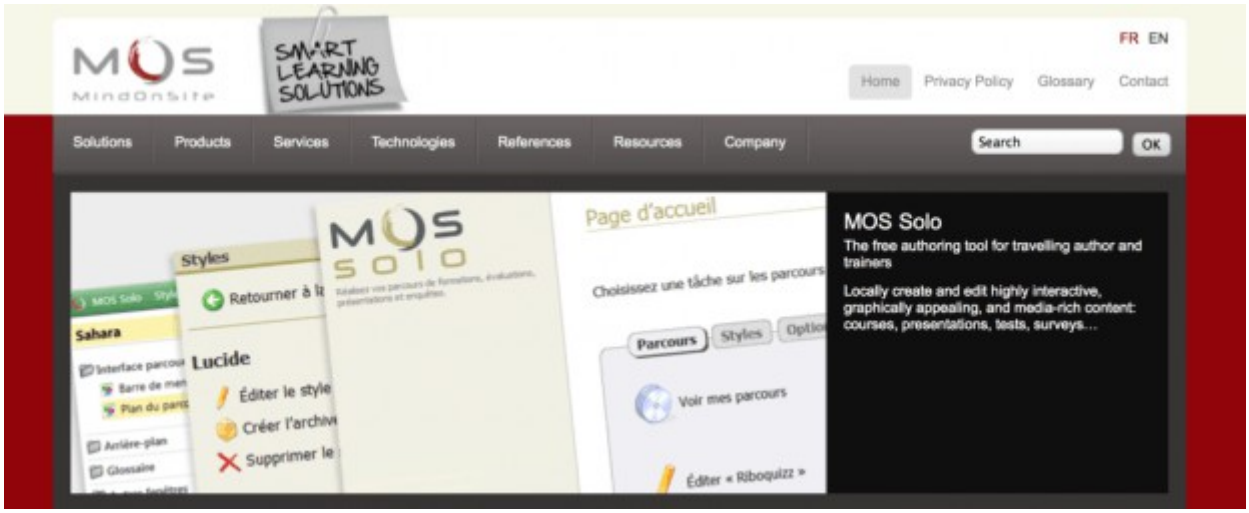


Рисунок 6 – Сайт MOS Sol

MOS Solo − простой, но функциональный инструмент, который практически не требует обучения, но представляет множество возможностей в создании мультимедийного образовательного контента. С помощью MOS Solo вы можете создавать интерактивные графические электронные курсы,

викторины, опросы и демонстрации. Внешний вид ресурса представлен на рисунке 6.

Рисунок 7 – Сайт Izzui

Izuui − это сервис для создания образовательных каналов на Facebook. Новая версия сервиса в настоящий момент находится в разработке − вы можете оставить свой e-mail, и вам придет уведомление о запуске сервиса. Пока вы можете посмотреть текущую версию Izzui. Внешний вид ресурса представлен на рисунке 7.

Рисунок 8 – Сайт Easygenerator

Easygenerator объединяет в себе простоту использования с мощностью и функциональностью, благодаря которым вы можете создать множество

разнообразных проектов и опубликовать их в Интернете или импортировать в Power Point. Внешний вид ресурса представлен на рисунке 8.

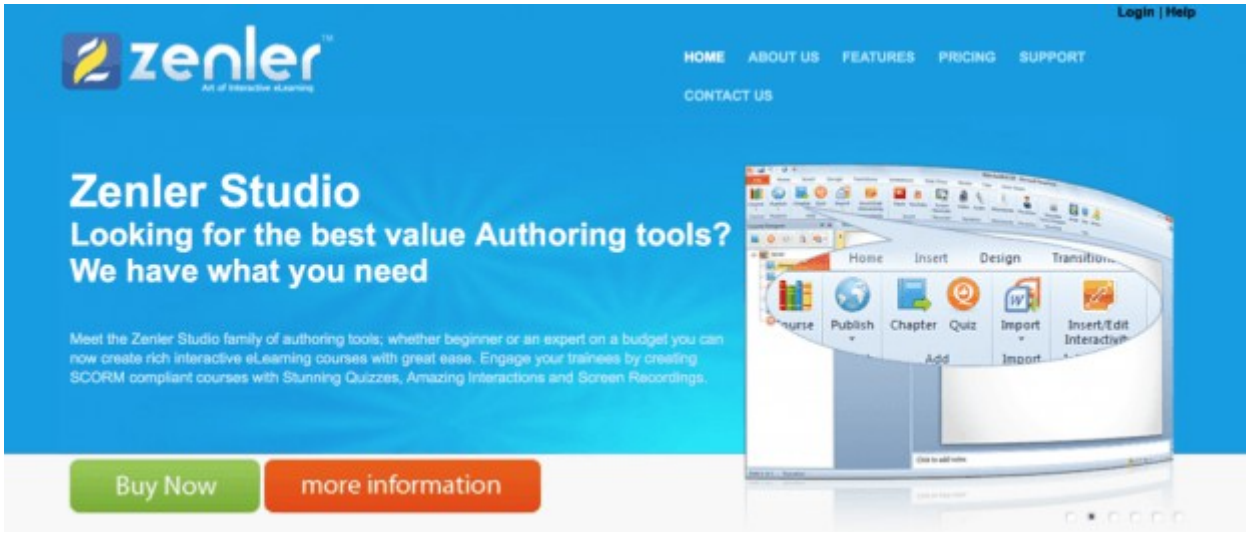


Рисунок 9 – Сайт Zenler

Zenler − это один из самых мощных сервисов для создания образовательного контента. С помощью Zenler вы можете создавать электронные курсы, которые будут работать где угодно, включая iPad, iPhone, Android. Вы даже сможете создавать курсы на основе ваших презентаций и материалов в PowerPoint. Сервис также позволяет записывать видео с экрана, добавлять аудио и многое другое. Основная версия Zenler платная, но вы можете скачать бесплатную пробную версию. Внешний вид сайта представлен на рисунке 9.

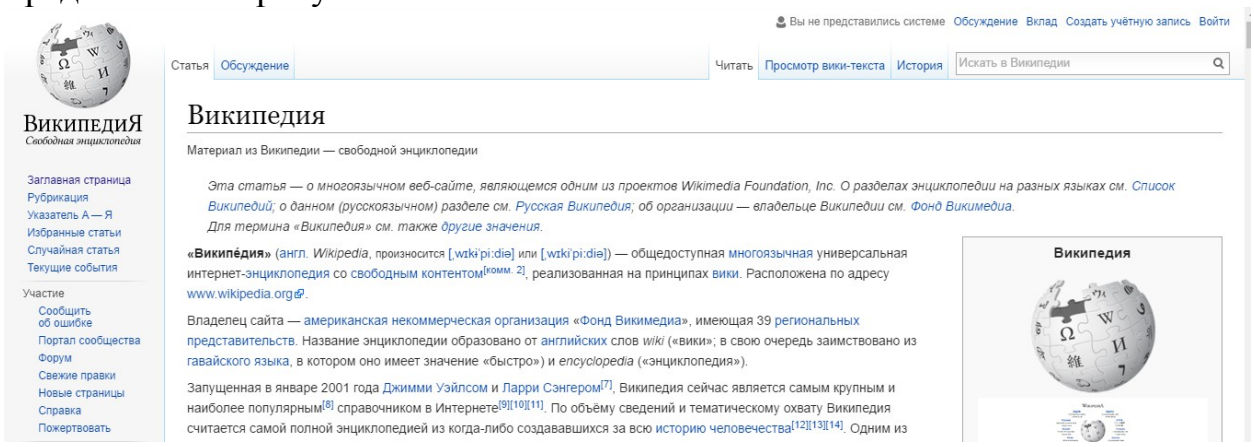


Рисунок 10 – Википедия — свободная энциклопедия

«Википедия» — общедоступная многоязычная универсальная интернет-энциклопедия со свободным контентом, реализованная на

принципах вики. Расположена по адресу www.wikipedia.org. Внешний вид энциклопедии представлен на рисунке 10.

Владелец сайта — американская некоммерческая организация «Фонд Викимедиа», имеющая 39 региональных представительств. Название энциклопедии образовано от английских слов wiki («вики»; в свою очередь заимствовано из гавайского языка, в котором оно имеет значение «быстро») и encyclopedia («энциклопедия»).

Запущенная в январе 2001 года Джимми Уэйлсом и Ларри Сэнгером, Википедия сейчас является самым крупным и наиболее популярным справочником в Интернете. По объёму сведений и тематическому охвату Википедия считается самой полной энциклопедией из когда-либо создававшихся за всю историю человечества. Одним из основных достоинств Википедии как универсальной энциклопедии является возможность представления информации на родном языке пользователя. На июнь 2016 года разделы Википедии есть на 295 языках, а также на 493 языках в инкубаторе. Она содержит более 40 миллионов статей. Интернет-сайт Википедии является седьмым по посещаемости сайтом в мире; в марте 2013 года его посетили более 517 миллионов человек.

Главной особенностью Википедии является то, что создавать и редактировать статьи в ней может любой пользователь Интернета. Все вносимые такими добровольцами изменения незамедлительно становятся видными всем посетителям сайта. В декабре 2013 года в заявлении ЮНЕСКО по случаю награждения Джимми Уэйлса, основателя Википедии, Золотой медалью Нильса Бора про Википедию было сказано, что она является «символом эпохи взаимодействия, в которую мы живём, и это не просто инструмент, это воплощение мечты, столь же древней, как человеческий интеллект и собрания Александрийской библиотеки».

Информационный сайт по информационной безопасности как образовательный ресурс при обучении сотрудников финансового предприятия. В отличие от других форм дистанционного обучения, информационный сайт вполне возможно воплотить в любом финансовом

предприятии, так как он не требует непосредственного контакта со специалистом по информационной безопасности, при необходимости связь может осуществляется через комментарии, не требует вложения больших средств в покупку и установку оборудования, создания различных центров обучения. Для реализации проекта нет необходимости устанавливать на сайт различные модули.

Создание HTML-справок дает возможность преподнести информационные материалы в самой удобной для изучения форме. HTML-справки можно формировать вручную или использовать для этого специализированное программное обеспечение.

Основная масса программного обеспечения для создания HTML-справок могут осуществлять более широкий спектр требований - формировать не только справки, но различные проектные материалы, картотеки, литературу и пр. Программное обеспечение для создания справок можно применять, когда нужно систематизировать весомый объем данных и подать его в наиболее привлекательной форме.

Методы создания справок

Существует возможность создать справку, не имея для этого специальных знаний и навыков. Для этого довольно создать страницы справки и содержание. Содержание это список тем, к которым можно быстро перейти, используя ссылки.

Наиболее часто применяемый метод реализовывается при создании HTML-справок - это применение фреймов (рамок). В данном случае в одну из рамок помещают заголовок HTML-справки, в другую - оглавление HTML-справки, в третью - само содержание HTML-справки. Преимущество данного метода оформления в том, что при просмотре страниц HTML-справки две первые рамки (с заголовком и содержанием) остаются без изменений и загружается только содержание HTML-справки, т.е. отдельные страницы.

Когда HTML-справка должна иметь много тем, подтем и страниц, указанные выше методы могут оказаться не совсем удачными, так как содержание HTML-справки начнет увеличиваться в размерах и существует возможность неудобного пользования.

Для объемных HTML-справок необходимо применять в качестве содержания раскрывающееся оглавление. А именно, при щелчке по разделу раскрывается дополнительный список подтем, при раскрывании подтемы - появляется перечень составляющих его страниц. Чаще всего для формирования HTML-справок достаточно использования трехуровневого раскрывающегося оглавления.

Для формирования раскрывающегося оглавления применяется код JavaScript. Можно изучить JavaScript и создавать код без посторонней помощи. Или можно применить специализированное программное обеспечение, способное создавать раскрывающееся оглавление в визуальном режиме, например Sothink DHTML Menu, Xara Menu Maker, Easy CSS Menu, HTML TreeView Generator и так далее.

Для этого необходимо вставить созданный специальной программой раскрывающееся оглавление на страницу - и содержание справки в целом готово (раскрывающееся оглавление сформировано в бесплатной программе HTML TreeView Generator).

Существует еще более простой способ создания справок - применить программное обеспечение, специально для этого предназначенное. В этом случае не нужно изучать html, css, javascript - работа во всех специальных программах по формированию справок ведется в онлайн режиме, и программа сама создает исходный код.

Ментальные карты (mind maps) и майндмэппинг (технология работы с ментальными картами) сегодня всё чаще рассматриваются в аспекте развития творческого мышления, личностных компетенций, умения излагать аргументированно свою точку зрения, творческой индивидуальности. Потенциал эксплуатации ментальной карты в обучающем процессе велик, выработка оптимальной методики майндмэппинга в электронных курсах позволяет лучше усвоить предлагаемый материал.

Применение ментальных карт для оживления мыслительного процесса описано в работах Тони Бьюзена, Хорста Мюллера, а также в ряде отечественных источников, которые преимущественно излагают идеи названных выше авторов, экстраполируя и интерпретируя их в новых

условиях практической реализации. Выступая одним из способов когнитивного видения, ментальные карты имеют несколько отличительных черт. А именно, специфика ментальных карт от разного рода логико-структурных схем состоит в свободной визуализации мыслительного процесса пользователя. Обобщая специфику ментальных карт, можно выделить следующие свойства.

Ментальные карты – это способ творческой визуализации мыслей пользователя.

Созданная ментальная карта может быть сходной с логическими схемами, или являться взаимосвязанными необычными яркими изображениями – исходя из пользовательского представления своего проекта.

При создании ментальных карт лучше не использовать готовые шаблоны, так как они провоцируют подгонять под них творческий процесс, тем самым подгоняя под определенные границы.

Изображаемые связи могут быть не только логическими, но ассоциативными, а данные – не только терминологическими, но и образными, приблизительными.

В Интернет-сети много различных материалов о ментальных картах и подавляющая часть описаний посвящена применению ментальных карт в экономике, в менеджменте, в бизнесе, в изобретательстве и так далее. На рисунках 11, 12 и 13, представлены соответствующие примеры ментальных карт, отражающие потенциал их использования.

Рисунок 11 – Mind map (ментальная карта) в обучении

Рисунок 12 – Применение интеллект-карт (ментальных карт)

Рисунок 13 – Сферы использования майндмэппинга

Из всех приведенных средств разработки электронных курсов во второй главе будут применены такие средства как сайт, ментальная карта, HTML-справка и вики-страница.

Глава 2. Создание цифрового контента для сопровождения информационной системы в предприятия

Создание сайта информационной безопасности для обучения сотрудников компании

Сайт - это цифровой контент, представляющий любую компанию или индивидуально представленного человека в Интернет сети. Также сайт представляет собой современную и передовую возможность передачи информации, являясь коммуникативным средством, и, наконец, рекламным продуктом, дающим большие возможности в области поиска и привлечения заинтересованных потребителей ресурсов.

Компетентная и качественная разработка, изготовление специализированного сайта решает сразу множество задач:

- обучение сотрудников правилам информационной безопасности;
- создание и укрепление стиля и имиджа;
- увеличение и расширение обучаемой аудитории;
- увеличение доходов фирмы или компании (за счет сокращения командировок);
- увеличение количества и качества передачи информации между компанией и сотрудниками.

Создание Web-сайтов является одной из важнейших технологий разработки ресурсов Интернет. Web-страница представляет собой текстовый файл с расширением *.htm, который содержит текстовую информацию и специальные команды - HTML-коды, определяющие, в каком виде данные будут отображаться в окне браузера. Вся графическая, аудио- и видео информация непосредственно в Web-страницу не входит и представляет собой отдельные файлы с расширениями (*.gif, *.jpg, *.mp3, *.avi и т.д.). Качественный сайт, содержащий в себе все полезные данные, является лучшей визитной карточкой и коммерческой фирмы и образовательных структур, работая на них круглосуточно.

Web-сайты дают возможность:

- анализировать спрос, мысли и выбор потребителей, кейс их знаний об определенных товарах, услугах и фирмах;

- формировать совместные проекты и курсы с отдаленной командой исполнителей;

- выполнять внутрифирменное повышение квалификации персонала или внутрикорпоративное обучение сотрудников предприятия;

- формировать коллективные приоритеты и нормы поведения, разъяснять политику, проводимую предприятием, облегчать взаимосвязь руководителей и сотрудников.

Цифровая среда имеет ряд очевидных плюсов и возможностей, среди которых:

- интерактивный характер коммуникации;
- постоянная доступность информации;
- постоянное обновление информации, дополнение с учетом запросов или предложений клиентов сайта;
- предоставление высоких объемов данных, а именно текстовой и графической, звуковой и видеоинформации.

В первой составляющей практической части представлен сайт, предоставляющий цифровой контент. По характеру предоставляемого цифрового контента - информационно-тематический.

Рисунок 14 - Структурная схема сайта.

Страница «Главная» описывает цель электронного курса по информационной безопасности и темы (рисунок 15).

Страница «Актуальность» рассказывает про развитие информационных технологий.

На странице «Основы информационной безопасности» находится необходимая к изучению информация. Там находятся ссылки на такие страницы как (рисунок 16):

- типы нарушителей;
- правила применения и хранения паролей;
- меры защиты ПК от несанкционированного доступа;
- использование мобильных средств связи;
- правила использования сотрудниками сети Интернет;
- функции администраторов информационной безопасности;
- обязанности сотрудников;
- ответственность.

Рисунок 15 – Внешний вид сайта.

Рисунок 16 – Подразделы курса информационной безопасности.

Благодаря данному сайту осуществлено цифровое взаимодействие между руководством компании и сотрудниками.

Ниже приведен фрагмент листинга сайта.

```
<!Doctype html>
<html>
<a name="top"></a>
<head>
<title>Основы информационной безопасности</title>
<meta http-equiv="Content-type" content="text/html; charset=windows-1251">
<script type="text/javascript" src="jquery-1.12.1.min.js"></script><style type="text/css"></style>
<link rel="stylesheet" type="text/css" href="style.css" media="all"/>
</head>
<body class="b-page">
   <div class="b-main_container">
<p class='h1'>Электронный курс по информационной безопасности</p>
          <nav class="b-head__menu">
              <ul>
<li class="menu-item menu-item-type-custom menu-item-object-custom menu-item-home menu-item-56"><a href="index.html" >Главная</a></li>
<li class="menu-item menu-item-type-post_type menu-item-object-page menu-item-55"><a href="relevance.html">Актуальность</a></li>
```

<li class="menu-item menu-item-type-post_type menu-item-object-page current-menu-item current_page_item menu-item-52">Основы информационной безопасности
 </nav>
</header>

<script type="text/javascript">
$(document).ready(function(){
 $('.spoiler_links').click(function(){
  $(this).parent().children('div.spoiler_body').toggle('normal');
  return false;
 });
});
</script>
Функции администраторов информационной безопасности
• Проведение работ с сотрудниками филиалов организации по соблюдению требований ИБ

• Контроль за соблюдением мер ИБ на рабочих местах сотрудников

♦ Соблюдение порядка физического доступа в производственные помещения офисов
♦ Выполнение условий в части отключения информационных ресурсов сотрудников офисов при их увольнении и/или переводе на другой участок работы
♦ Удаление конфиденциальной информации с жесткого диска при их передаче на склад или другое помещение
♦ Контроль за соблюдением в офисе основных мер по ИБ. Информирование руководства офиса и службы информационной безопасности о выявленных недостачах в части обеспечения безопасности информационных технологий


```
&bull;<a href="" class="spoiler_links"> Организация и контроль доступа к информационным ресурсам</a>
 <div class="spoiler_body">
 &diams; Подготовка заявок на предоставление прав доступа к информационным ресурсам сотрудникам офисов в соответствии с принципом минимизации прав, достаточных прав для выполнения функциональных обязанностей <br>
&diams; Ведение учета ресурсов, доступ к которым предоставляется сотрудникам подразделения <br>
&diams; Рассмотрение и согласование с руководством своего офиса заявок от других офисов на доступ к информационным ресурсам своего подразделения <br>
&diams; Взаимодействие с администратором сервера либо автоматизированной системы при необходимости осуществления разблокировки учетной записи пользователя офиса. Выяснение причины блокировки учетной записи пользователя <br>
</div>
</div>
<p>&bull; Участие в проведении информационного обследования в филиалах организации, подготовка необходимых материалов</p>
<p>&bull; Проведение работ с сотрудниками офисов по соблюдению требований ИБ </p>
<p>&bull; Инструктаж сотрудников по общим вопросам обеспечения ИБ, в том числе антивирусной защиты, в офисах организации </p>
<p>&bull; Обучение сотрудников с перечнем конфиденциальной информации, обрабатываемой в организации, которая будет доступна им в ходе выполнения функциональных обязанностей </p>
<p>&bull; Ознакомление сотрудников с ответственностью за нарушение ИБ </p>
<br>
                                <div class='img'>
                    <img src="img/ib1.jpg" >
            </div>
            <br>
<p><b>Подразделы:</b>
<br>
&bull; <a href="perpetrators.html" >Типы нарушителей </a>
```

```
<br>
&bull; <a href="passwords.html" >Правила применения и хранения паролей </a>
<br>
&bull; <a href="media.html" >Меры защиты ПК от несанкционированного доступа </a>
<br>
&bull; <a href="communication.html" >Использование мобильных средств связи </a>
<br>
&bull; <a href="employees.html" >Правила использования сотрудниками сети Интернет </a>
<br>
&bull; <a >Функции администраторов информационной безопасности </a>
<br>
&bull; <a href="duties.html" >Обязанности сотрудников </a>
<br>
&bull; <a href="responsibility.html" >Ответственность </a>
</p>
<div class='bottom'>
<a href="#top" >К началу страницы</a>
<a href="basics.html" >К началу раздела</a>
<a href="#" onclick="history.back();">Назад</a>
</div>
    <div id='footer'>
        <br>
Copyright © 2016 by Ольга Карагодина. All Rights Reserved.
    </div>
  </div>
        </div>
</body>
</html>
```

Создание ментальной карты

Важным средством представления информации являются ментальные карты. На данный момент лучшим средством для создания ментальных карт, является сервис mindomo.com. Сервис mindomo организован на высоком, интуитивно доступном для пользователя уровне. Ленточная панель

управления напоминает Mocrosoft Office, что значительно облегчает освоение сервиса и создание ментальной карты. Ментальная карта памяти - это диаграмма, которая знакомит пользователя сервиса с концепцией, назначением или другими объектами, связанными и расположенными вокруг ключевых слов, идеи или плана. Эти карты используются для формирования, представления информации, структурирования идеи, как вспомогательные средства в учебе, организациях, решении проблем и принятия решений. При использовании методов работы с картами памяти, выявляются явные плюсы:

- карты памяти помогают легко запомнить информацию, так как она структурирована;
- карты памяти облегчают визуальное восприятие и понимание вопроса, существует возможность вставки рисунков и заметок;
- карты памяти раскрывают информацию, под каждой темой можно создавать подтемы и после просмотра общей картины перейти к более детальному изучению вопроса.

Сервис Mindomo это идеальный вариант для создания цифрового контента, так как позволяет создать карту памяти на безвозмездной основе, не скачивая и не предустанавливая программное обеспечение, работать с сервисом можно онлайн. Для работы или ознакомления с приложением необходимо перейти на официальный сайт http://m.mindomo.com/

Каждая публичная карта, созданная Mindomo, имеет уникальный адрес, который можно использовать на страницах HTML, чтобы указать ссылку на необходимую карту или пригласить других пользователей к совместной работе. Можно связывать карты со своей домашней страницей или отправить их другим пользователям для ознакомления, приглашение направляется по электронной почте.

Преимущества работы с Mindomo.

Более эффективное управление и сохранение информации.

Более эффективная коммуникативная информация.

Улучшение творческого мышления и обучения пользователей.

Распознавание направлений, кластеров и других моделей в представленной информации.

Обобщение разрозненных фрагментов информации в систему.

Еще одно преимущество, например по сравнению с однообразным текстом, использования Mindomo заключается в том, что есть бесплатный допуск в библиотеку карт памяти, которая поможет учиться у других пользователей - авторов карт памяти, как использовать методы работы с картами памяти в другом программном обеспечении и сервисах.

Создание карт памяти позволяет визуально сохранять сложные концепции, задачи, методы, технические задания и другую взаимосвязанную информацию в структурированном представлении. Темы связаны между собой линиями. Также как и контур в структуре, каждая тема имеет большое количество подзаголовков, содержащих текст, примечания, ссылки и графику, позволяя виртуально представлять информацию любого вида.

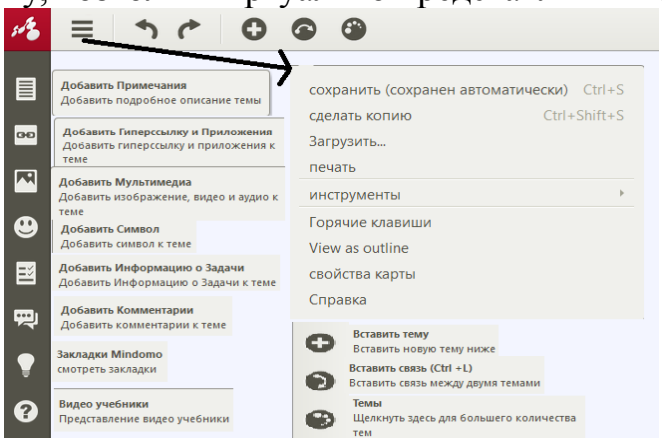


Рисунок 17 – Функциональность.

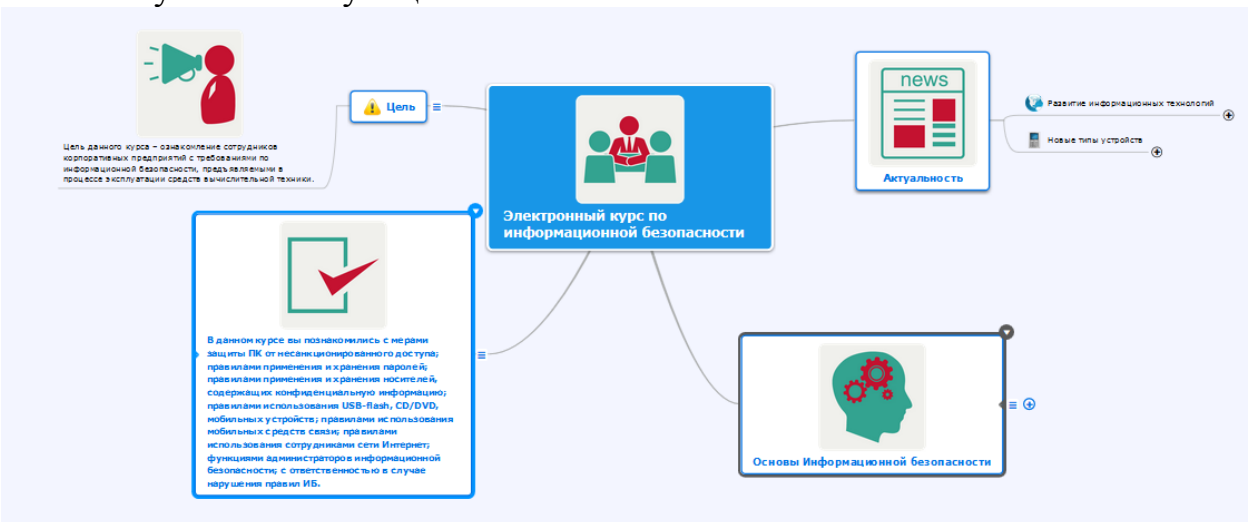


Рисунок 18 – Основные блоки ментальной карты.

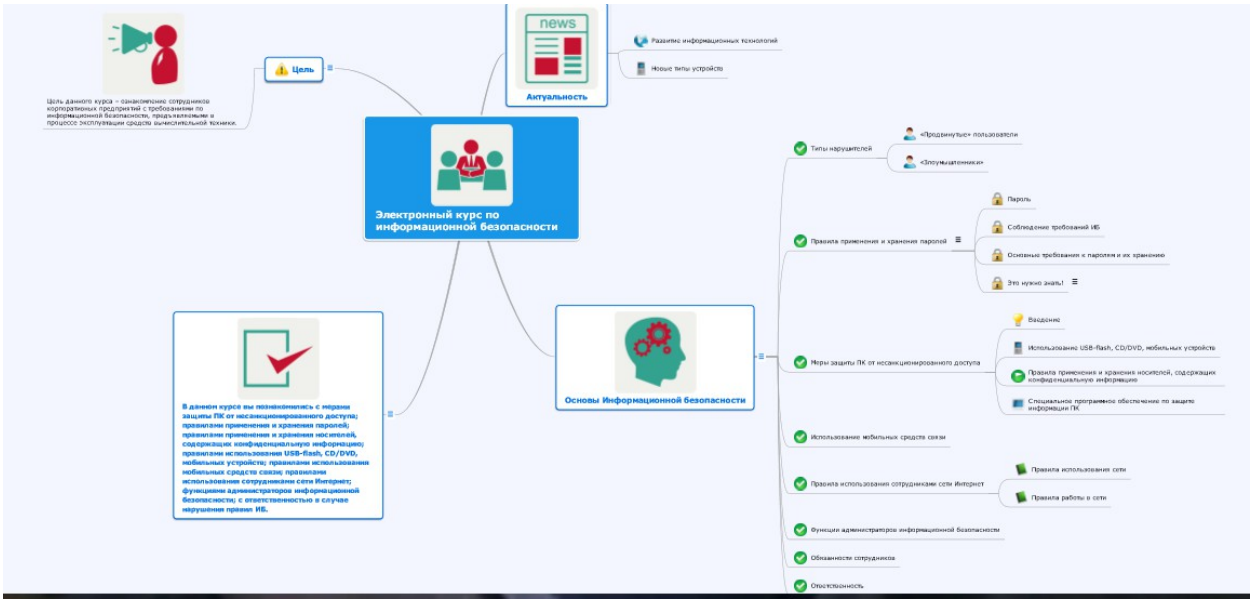


Рисунок 19 – Ментальная карта.

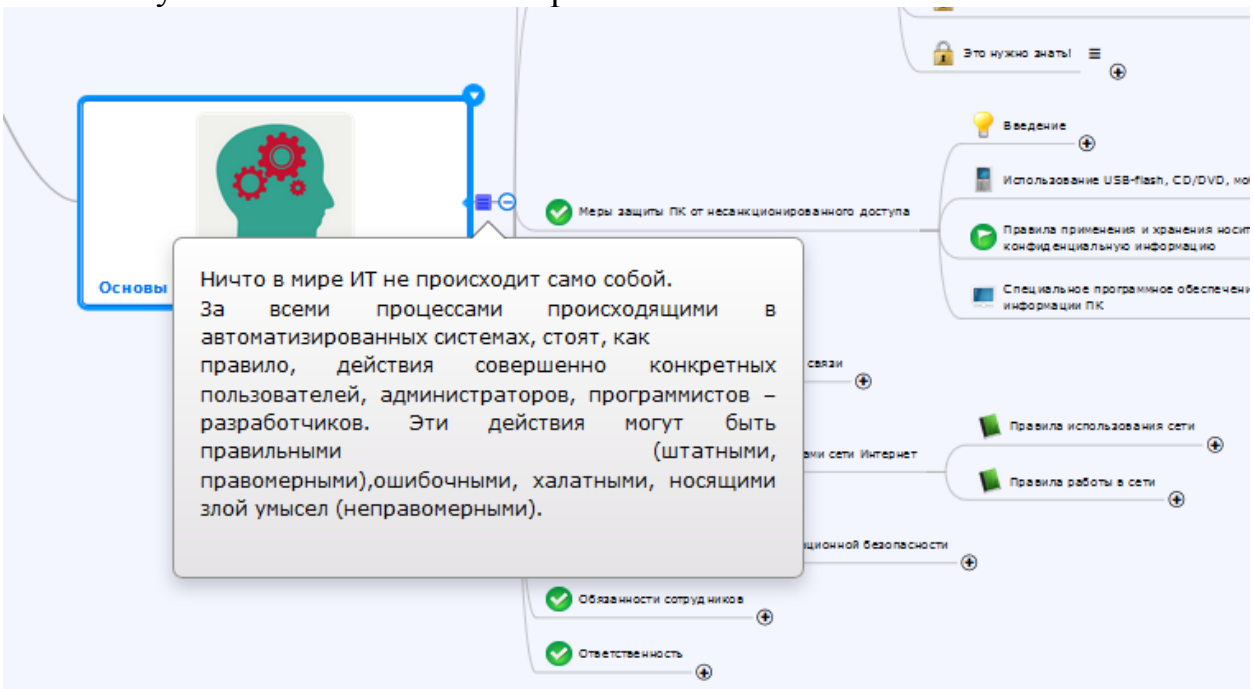


Рисунок 20 – Заметки в ментальной карте.

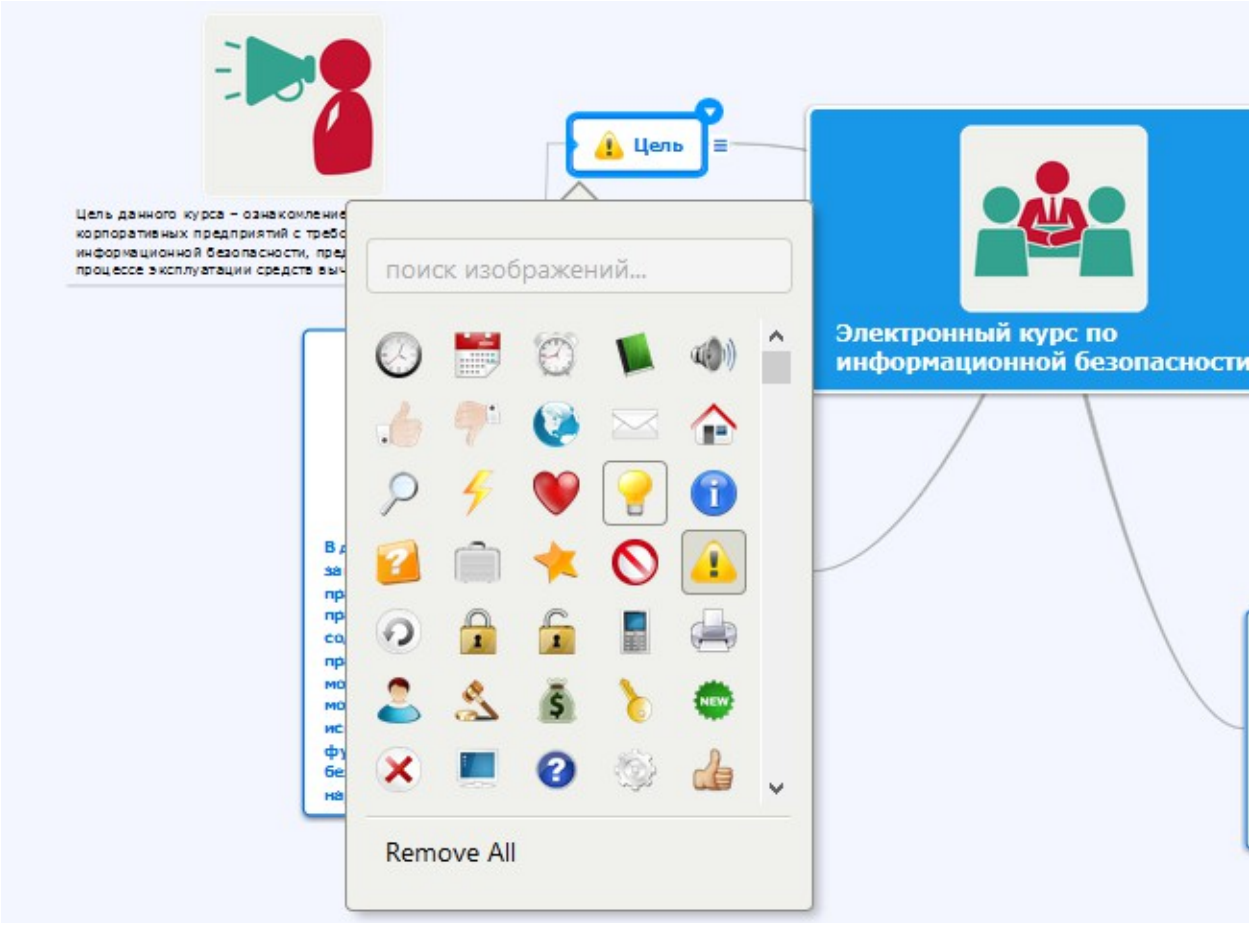


Рисунок 21 – Возможность вставки рисунков в темы ментальной карты

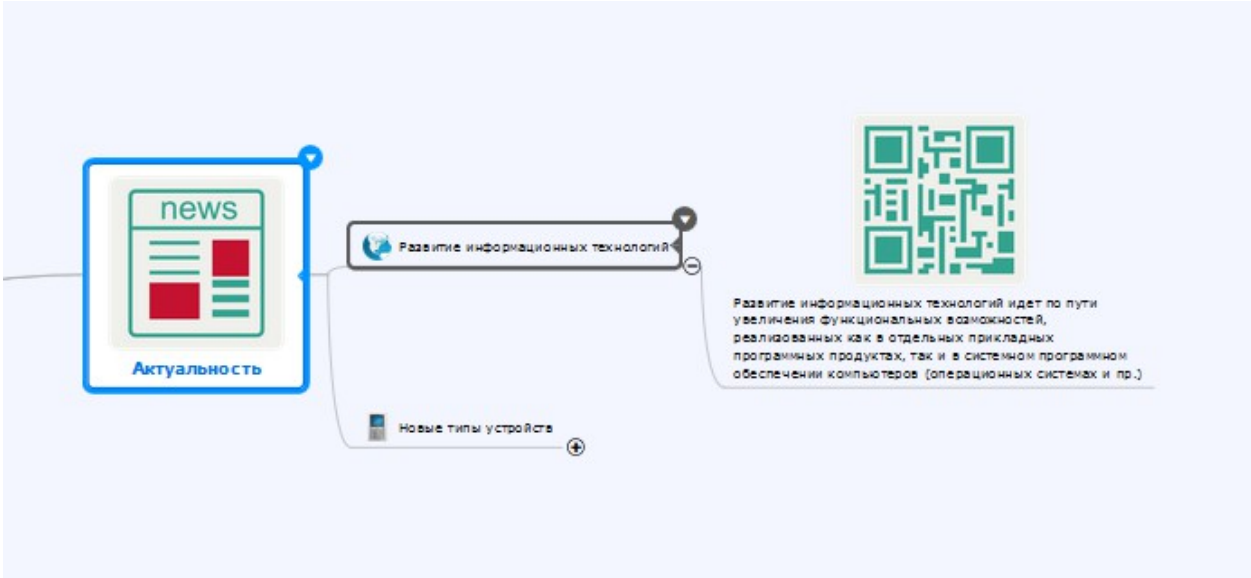
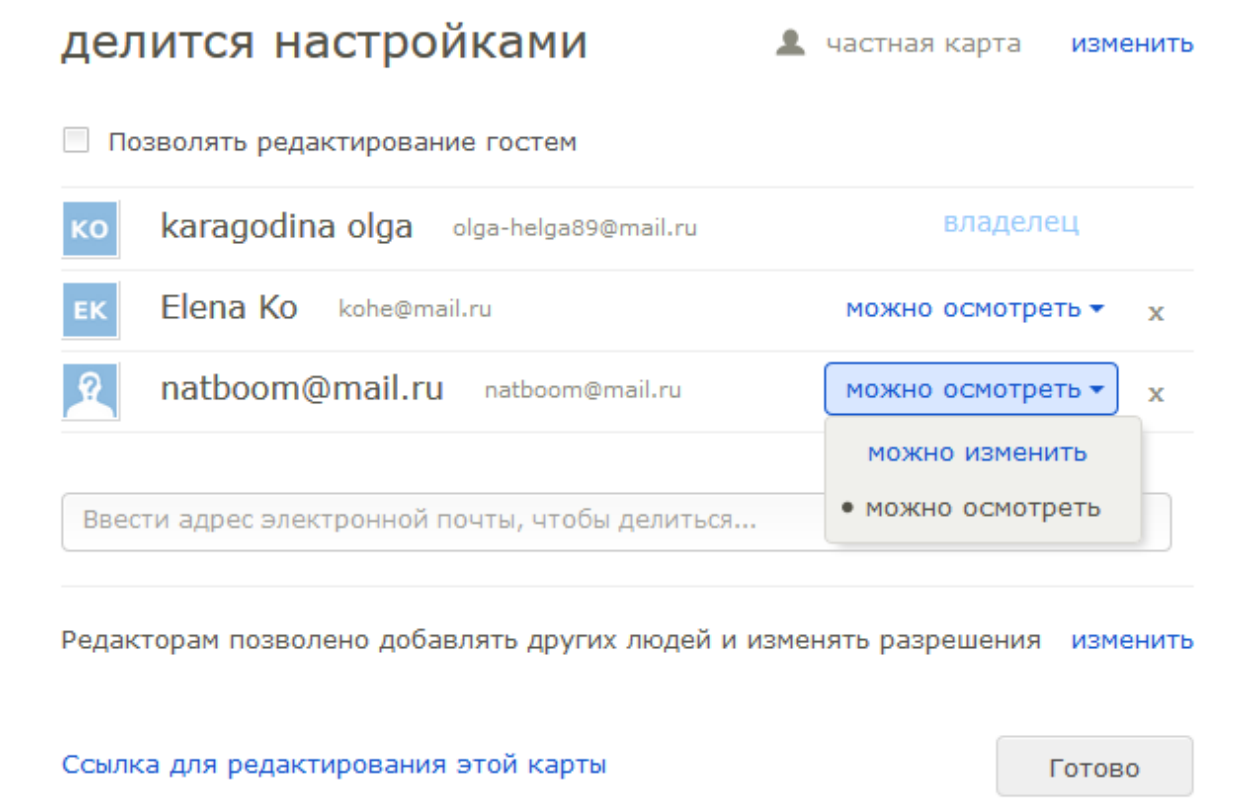


Рисунок 22 – Возможность просмотра отдельных тем в ментальной карте

Рисунок 23 – Возможность совместного редактирования в ментальной карте



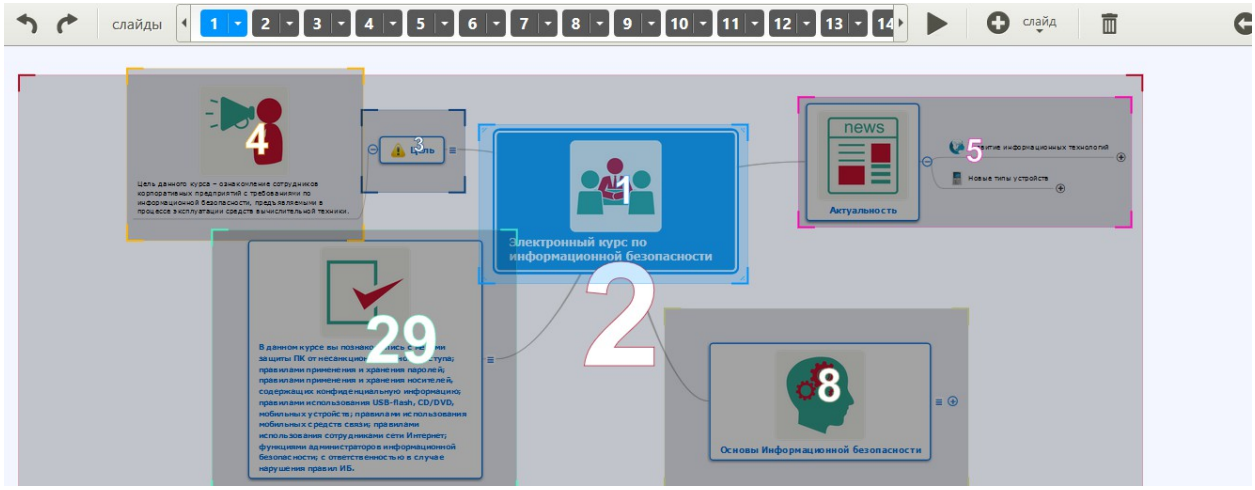


Рисунок 24 – Возможность создания видео-презентации в ментальной карте

Создание Вики-страницы

Вики — это технологии мгновенного создания гипертекстовых страниц в Интернете или на сервере локальной сети, что позволяет не только

просматривать страницы вики-сайта, но и корректировать их, создавать новые, размещать в сети свои документы самых разных форматов. Как правило, в Вики доступны обсуждения, связанные с публикуемой информацией, а также сохраненная история всех производимых изменений. Изучив интуитивно понятный язык разметки вики-страниц, можно размещать в открытом доступе цифровые обучающие курсы, организовывать обсуждения по разным вопросам, привлекать коллег к независимой работе по разработке элеткронных курсов или проектов.

Вики-движо́к — программное обеспечение для организации вики — веб-сайта, контент который создают сами пользователи, используя любой браузер. Обычно вики-движок является веб-приложением, выполняемом на одном или нескольких серверах. Контент, включая всю историю правок, хранится в базе данных или файловой системе. Существует множество вики-движков, написанных на различных языках программирования, включая открытое и проприетарное программное обеспечение.

Существует три основных типа использования технологии вики: публичные вики, создающиеся сообществом читателей; частные корпоративные вики, используемые для хранения документации, и личные, используемые в качестве дневника или блога.

Публичные вики. Доступ к публичной вики имеет каждый пользователь, часто (но не всегда) для совершения правок не требуется регистрация. Большинство таких вики созданы на базе движка MediaWiki. Ярким примером является — Википедия.

Корпоративные вики. Корпоративные вики используются для хранения документации и обмена знаниями между сотрудниками. Многие компании и правительственные организации используют вики — Adobe Systems, Amazon.com, Intel, Microsoft.

Персональные вики. Также предназначены для организации дневников и блогов.

Основные элементы форматирования текста

Таблица 1 – Вики-страницы

На странице	Исходный текст (язык Вики

Вики поддерживает жирный, курсивный, подчеркнутый и моноширинный текст. Можно объединять элементы оформления.	Вики поддерживает **жирный**, //курсивный//, __подчеркнутый__ и "моноширинный" текст. Можно **__// "объединять"//__** элементы оформления.
Можно набирать текст в нижнем и верхнем индексе.	Можно набирать текст в _{нижнем} и ^{верхнем} индексе.
Можно помечать текст как удаленный.	Можно помечать текст как ~~удаленный~~.

Абзацы разделяются пустыми строками. Необходимо оставить пустую строку там, где один абзац вы хотите отделить от другого. Если нужно вставить разрыв строки без создания нового абзаца, используйте две обратные косые черты и пробел (или перевод строки) после них.

Ссылки внутри Вики создаются с помощью двойных квадратных скобок. Если вам нужно сослаться на некоторую страницу (например, playground) в вашем пространстве имен, то просто укажите: [[playground]].

Для структурирования текста на странице можно использовать заголовки пяти уровней вложенности. Если использовать более трех заголовков первых трех уровней, автоматически создается список содержимого страницы (отображается вверху как «Содержание»). Чтобы отключить эту функцию (например, когда текст страницы умещается в один экран), нужно включить в текст страницы неотображаемую строку: ~~NOTOC~~

С помощью четырех и более минусов (дефисов) можно сделать горизонтальную разделительную линию.

Таблица 2 – Редактирование текста

Как это выглядит	**Что нужно набрать**

Начните раздел со строки заголовка: Новый раздел **Подраздел** **Подподраздел**	Начните раздел со строки заголовка: == Новый раздел == === Подраздел === ==== Подподраздел ====
Одиночный перевод строки не влияет на разметку. Его можно использовать, чтобы разделять предложения в одном абзаце. Некоторые редакторы считают, что это облегчает редактирование и улучшает функцию *сравнения версий*. Но пустая строка начинает новый абзац.	Одиночный перевод строки не влияет на разметку. Его можно использовать, чтобы разделять предложения в одном абзаце. Некоторые редакторы считают, что это облегчает редактирование и улучшает функцию "сравнения версий". Но пустая строка начинает новый абзац.
С помощью тега «br» можно разрывать строки, не начиная новый абзац.	С помощью тега «br» можно разрывать строки, не начиная новый абзац.
Сделать список очень просто: • каждая строка начинается со звёздочки; ○ чем больше звёздочек — тем глубже уровень; отступ внутри можно делать и с помощью двоеточия.	Сделать список очень просто: * каждая строка начинается со звёздочки; ** чем больше звёздочек — тем глубже уровень; **: отступ внутри можно делать и с помощью двоеточия.

1. Нумерованные списки тоже хороши:
  1. очень организованные;
  2. легко читаются.
	# Нумерованные списки тоже хороши:
	## очень организованные;
	## легко читаются.

• Можно также делать смешанные списки: 1. и вкладывать их	* Можно также делать смешанные списки: *# и вкладывать их *#* как, например,

▪ как, например, 2. здесь.	*# здесь.
Точка с запятой в начале строки и затем двоеточие создают двухуровневый список.	; Точка с запятой в начале строки : и затем двоеточие ; создают : двухуровневый список.
Двоеточие в начале строки делает отступ абзаца. Простой перенос строки при этом начинает новый абзац. Примечание: это применяется в основном на страницах обсуждения.	: Двоеточие в начале строки делает отступ абзаца. Простой перенос строки при этом начинает новый абзац.
ЕСЛИ строка начинается с пробела, ТОГДА она будет отформатирована так же, как и набрана; шрифтом фиксированной ширины; без переноса строк; [[без ссылок]]; КОНЕЦЕСЛИ Это можно применять для: * вставки преформатированного текста; * описания алгоритмов; * исходного кода программ * ascii art (создание изображений при помощи текстовых символов). **ВНИМАНИЕ!** Если вы сделаете такую строку длинной, у неё появится полоса прокрутки. Никогда не начинайте обычные строки с пробела.	ЕСЛИ строка начинается с пробела, ТОГДА она будет отформатирована так же, как и набрана; шрифтом фиксированной ширины; без переноса строк; [[без ссылок]]; КОНЕЦЕСЛИ Это можно применять для: * вставки преформатированного текста; * описания алгоритмов; * исходного кода программ * ascii art (создание изображений при помощи текстовых символов);
Центрированный текст.	Центрированный текст.
Горизонтальная разделительная линия: четыре дефиса подряд	Горизонтальная разделительная линия: ---- четыре дефиса подряд

Этот абзац отцентрирован. Этот абзац выровнен по левому краю. Этот абзац выровнен по правому краю.	Вы можете управлять выравниванием текста абзаца, используя теги с указанием в атрибуте style параметра text-align, со значением • center для выравнивания по центру, • left для выравнивания по левому краю, • right для выравнивания по правому краю. По умолчанию принято выравнивание по левому краю. Например, для выравнивания по правому краю используйте такую конструкцию: Текст

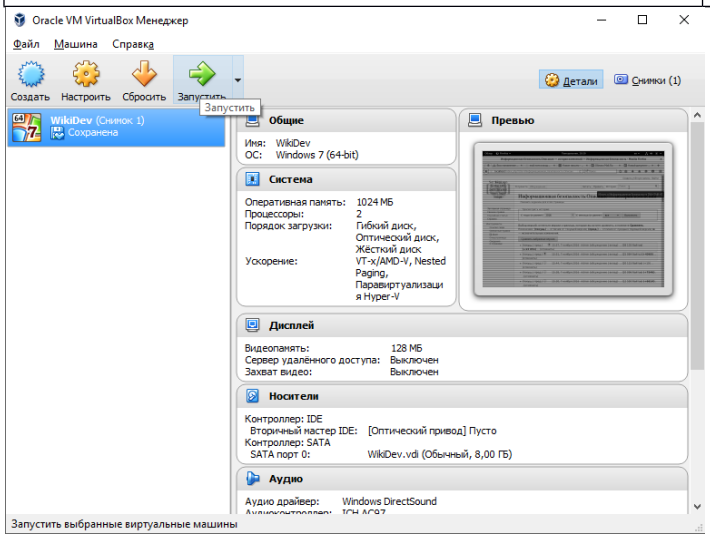


Рисунок 25 – Запуск Вики-движка

На рисунке 25 представлен запуск Вики-движка виртуальной машине.

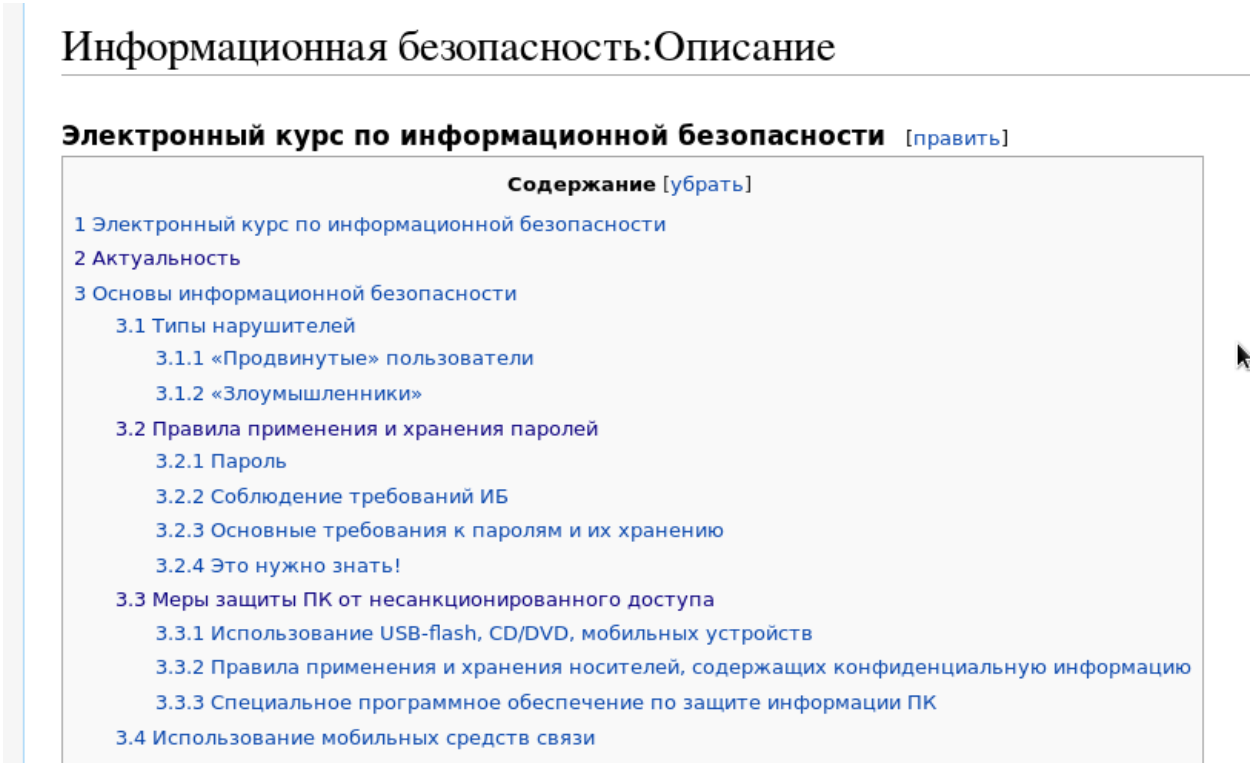


Рисунок 26 – Вики-страница содержание

На рисунке 26 представлена сформированная электронная страница по обучению читателей основам информационной безопасности.

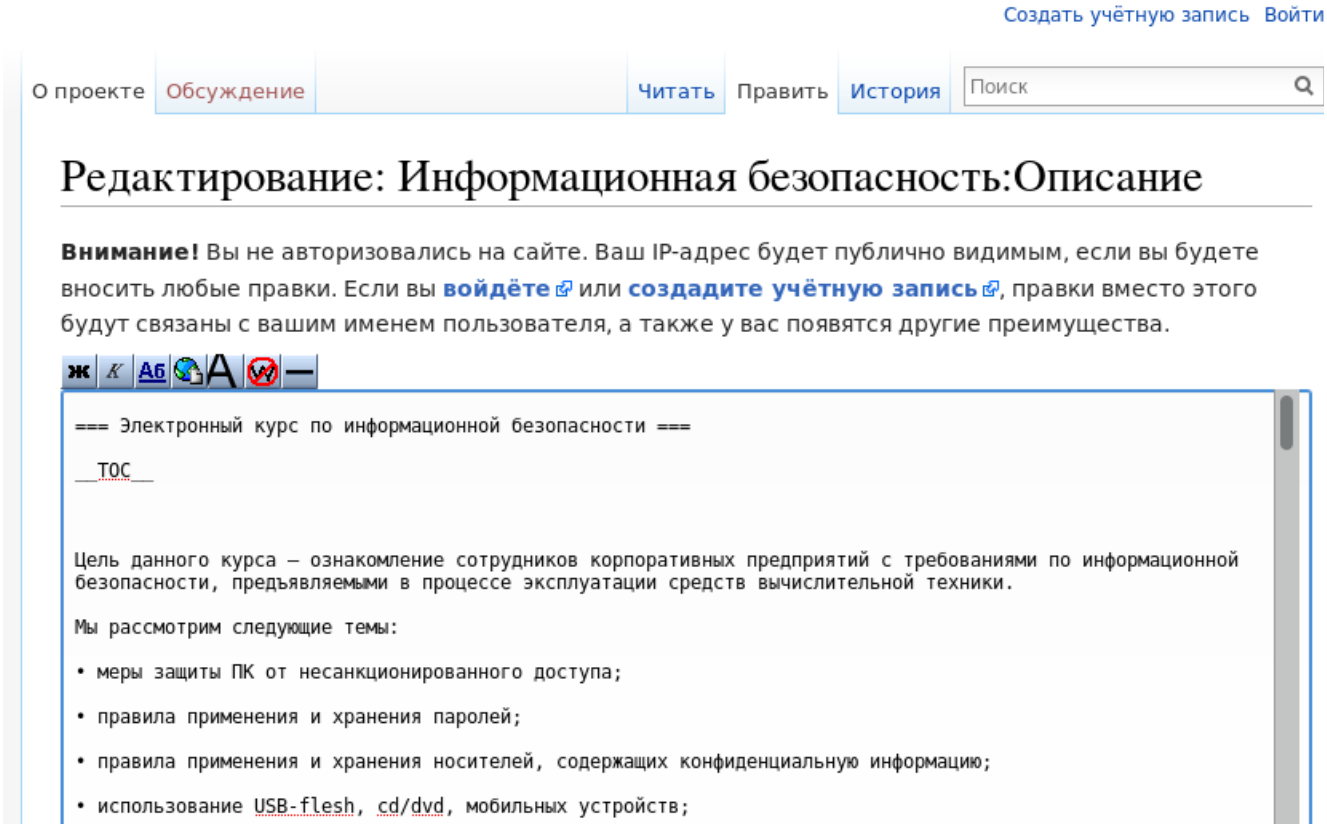


Рисунок 27 – Вики-страница правка

На рисунке 27 представлена возможность правки электронного курса.

Создание HTML-справки

Файл справки CHM (Microsoft Compressed HTML Help, Microsoft Compiled HTML Help) или скомпилированный HTML файл - это проприетарный формат файлов (от англ. proprietary software; от proprietary — частное, патентованное, в составе собственности и software — программное обеспечение) контекстной справки, разработанный корпорацией Microsoft и выпущенный в 1997 году в качестве замены формата WinHelp. Содержит в себе набор HTML-страниц, может включать в себя содержание со ссылками на страницы, предметный указатель, а также базу для полнотекстового поиска по содержимому страниц, что является сильной стороной этого формата. Все входящие в CHM файлы сжаты алгоритмом LZX.

Для просмотра CHM-файлов используется стандартное средство просмотра, встроенное во все версии Microsoft Windows, начиная с Windows 98, и Windows NT. Кроме того, существует ряд сторонних программ-просмотровщиков (FBReader и другие). Файл справки или файл помощи в формате CHM - это набор веб-страниц, сжатых и скомпилированных в единый файл. Сейчас одним из самых популярных форматов файлов справки для приложений является именно CHM. Файл справки в формате CHM является самым подходящим средством для быстрого создания контекстной помощи для нашего электронного курса.

Описание электронного курса.

При разработке курсов всегда важно посмотреть на удобство использования не столько со стороны разработчика, сколько со стороны конечного пользователя: логичность и простоту навигации, полезность для пользователя. Часто создаются такие продукты, которые содержат ценную информацию, полезные знания, но слушатель должен пробираться через неочевидные навигационные кнопки, лишние баннеры, не работающие ссылки. Тем самым мы на корню можем убить все желание к получению знаний.

Для открытия электронного курса по информационной безопасности сделайте следующее: дважды щёлкните по файлу или щёлкните правой

кнопкой мыши по файлу «Электронный курс по информационной безопасности» и выберите «Открыть»;

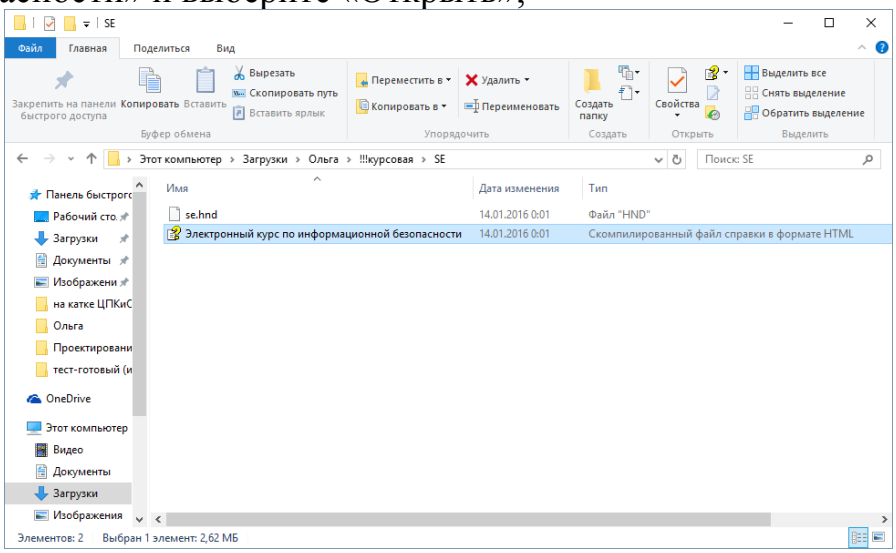


Рисунок 28 - Внешний вид файла справки

Можно просматривать справку по темам. Нажмите кнопку Содержание слева в меню справки и щелкните один из заголовков появившегося списка. Заголовок темы может содержать раздел справки или заголовки других тем. Щелкните раздел справки, чтобы открыть его, или другой заголовок, чтобы перейти к разделу нижнего уровня (Рис. 29).

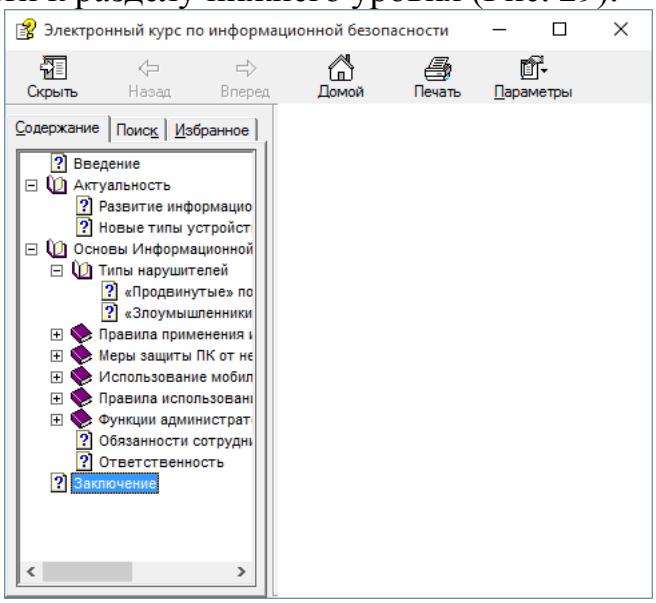


Рисунок 29 - Содержание файла справки

Созданный файл справки по ИБ структурирован, содержит текстовую, графическую информацию (Рис. 30).

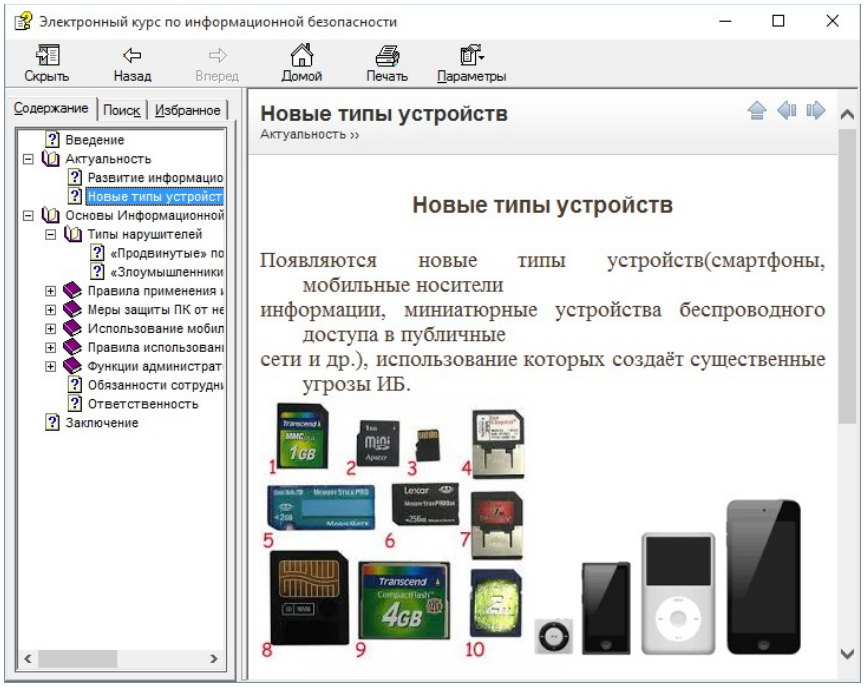


Рисунок 30 - Внешний вид отображения информации

Также для переключения можно воспользоваться не содержанием, а стрелками для переключения на следующую тему (Рис. 31).

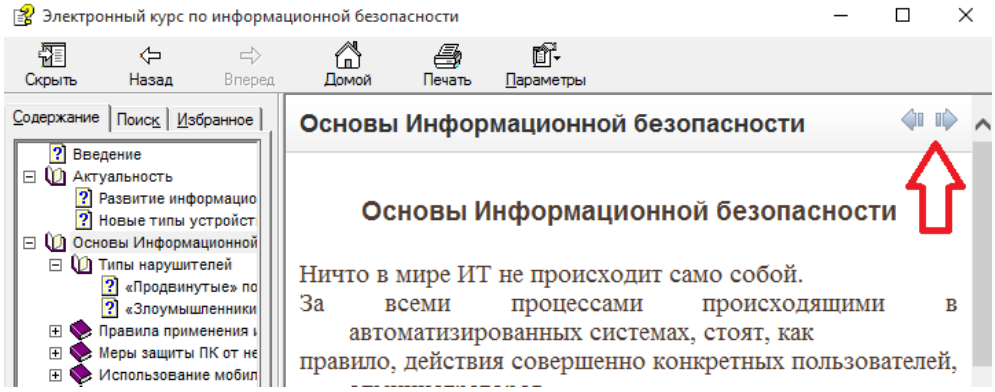


Рисунок 31 - Возможность перехода между темами

Глава 3. Экономическая часть

Результаты данного дипломного проекта могут быть использованы при обучении сотрудников финансового предприятия основным правилам по информационной безопасности. Введение данной программы позволит более точно вести прием данных, а так же влечет за собой экономию времени и средств при расчетах. Назначением данного дипломного проекта является повышение эффективности деятельности предприятия.

Расчет экономической эффективности проекта производится до начала проектирования и разработки системы, то есть в результате мы получаем расчет потенциального эффекта от внедрения системы на предприятии/

На созданный цифровой контент имеются заказы от нескольких финансовых предприятий.

Данная программа очень проста в применении, что позволяет значительно сократить затраты времени на обучение кадров.

Данная программа имеет очень скромные системные требования, занимает мало места на диске.

Для разработчика информационной системы источником дохода является продажа электронных курсов заказчикам. Затраты включают в себя затраты на разработку и тиражирование системы. Источником финансирования являются собственные средства разработчика.

Для финансового предприятия-заказчика источником экономии выступает замена ручного труда машинным, что в значительной степени сокращает время проведения расчетов. Затраты предприятия складываются из единовременных затрат на приобретение информационной системы, ее транспортировку и внедрение, а так же затрат, непосредственно связанных с проведением анализа и сопровождением системы.

Определение затрат на создание цифрового контента.

Были определены статьи затрат и нормы расхода по ним для последующего включения в расчет себестоимости программного продукта.

- на вспомогательные материалы, включающие: тонер для картриджа, бумага для принтера, диски, дискеты, память USBFLASHDRIVE и т.п. (таблица 1);

- на электроэнергию, учитывая мощность потребляемой энергии компьютера, принтера и т.п. устройств;
- на основную и дополнительную заработную плату разработчика программного продукта;
- отчисления на социальные нужды;
- накладные расходы (укрупнено);

Расчет себестоимости программного продукта

Себестоимость программного продукта рассчитывается по формуле (1):

$$C = M_{вс} + Э + З^{о}_{зп} + З^{д}_{зп} + З_{сн} + H , \quad (1)$$

где $M_{вс}$ - затраты на вспомогательные материалы, р.;

$Э$ - затраты на электроэнергию на технологические цели, р.;

$З^{о}_{зп}$ - основная зарплата разработчика, р.;

$З^{д}_{зп}$ - дополнительная зарплата разработчика, р.;

$З_{сн}$ - взносы на социальное страхование и обеспечение, р.;

H - накладные расходы, р.

Затраты на вспомогательные материалы приведены в таблице (1).

Таблица 1 - Затраты на вспомогательные материалы

Наименование затрат	Количество, шт.	Сумма, р.
1. Тонер для картриджа SamsungSCX-4200 (110 гр., Тонер B&W LI-463)	1	210
2. Упаковка бумаги для принтера (500 лист.)	1	228
3. Диск VSCD-R 700 Mb	1	45
4. Память USB Flash Silicon Power Helios 101 8 Гб	1	230

Итого:	713

Затраты на электроэнергию рассчитываются по формуле (2):

$$Э = P \cdot C_э \cdot T_{ОБЩ} \cdot R_{заг}, \quad (2)$$

Где

P - мощность потребляемой электроэнергии, кВт;

$C_э$ - стоимость одного киловатт-часа электроэнергии, р./кВт-ч;

$T_{ОБЩ}$ - общие затраты труда на разработку программного продукта, час;

$R_{заг}$ - коэффициент загрузки компьютера.

Подставив в формулу (2) числовые значения вычислим затраты на электроэнергию:

$Э=0,5 \cdot 1,92 \cdot (15 \cdot 8) \cdot 0,6=69,12$ *р.*

Основная заработная плата разработчика рассчитывается по формуле (7):

$$З^{о}_{зп}=C_{чтс} \cdot T'_{ОБЩ}, \quad (3)$$

где

$C_{чтс}$ - часовая тарифная ставка разработчика, р./час;

$T_{ОБЩ}$ - общие затраты труда на разработку программного продукта, час.

Подставив в формулу (3) числовые значения вычислим основную заработную плату разработчика:

$З^{о}_{зп}$=30·(15·8)=3600 *р.*

Взносы на социальное страхование и обеспечение определяются по формуле (8):

$З_{сн}=(З^{о}_{зп}+З^{д}_{зп})\cdot R_{сн}$, (4)

где $R_{сн}$ - коэффициент взносов на социальное страхование и обеспечение, $R_{сн}$ = 0,30.*(ПФ – 22%, ФСС – 2,9%, ФОМС – 5,1%)*

Подставив в формулу (4) числовые значения, вычислим взносы на социальное страхование и обеспечение:

$З_{сн}$=(3600)·0,30=1080 *р.*

Накладные расходы рассчитываются по формуле (4):

$Н=0,1\cdot(З^{о}_{зп}+З^{д}_{зп})$, (4)

Подставив числовые значения в формулу (4), получим:

Н= 0,1·(3600)=360 *р.*

Полная себестоимость разработанного программного продукта:

С=713+69,12+3600+1080+360=5822,12 *р.*

В таблице (2) сведены результаты расчетов себестоимости программного продукта.

Таблица 2 - Калькуляция себестоимости программного продукта

Наименование статей расходов	Затраты, р.

1	2
1. Основная заработная плата разработчика	3600
2. Взносы на социальное страхование и обеспечение	1080
3. Накладные расходы	360
4. Затраты на электроэнергию	69,12
5. Вспомогательные материалы	713
6. Полная себестоимость программного продукта	5822,12

В таблице (3) приведена стоимость электронных курсов по информационной безопасности от различных компаний. Исходя из данных данной таблицы можно сделать вывод, что проект реализуем и эффективен. Срок окупаемости программы будет достигнут на третьем месяце реализуемого проекта

Название курса	**Длительность**	**Цена**	**Вендор**	**Форма обучения**
Применение технологии управления правами AD RMS для защиты документов	1 день	2 000	Учебный центр Информзащита	Электронный курс
Организация непрерывности ведения и восстановления бизнеса	1 день	2 000	Учебный центр Информзащита	Электронный курс
Повышение осведомленности персонала в области действия стандарта PCI DSS 2.0	1 день	2 000	Учебный центр Информзащита	Электронный курс
Повышение компетенции персонала в области борьбы с мошенничеством	1 день	2 000	Учебный центр Информзащита	Электронный курс
Повышение осведомленности сотрудников компании в	1 день	2 000	Учебный центр Информзащита	Электронный курс

вопросах информационной безопасности				
Основы информационной безопасности для пользователей	1 день	3000	Академия АЙТИ	Электронный курс
Разработка политик информационной безопасности и программ повышения компетенции персонала	2 дня	24000	Сетевая Академия Ланит	Электронный курс + политика по информационной безопасности
Повышение осведомленности сотрудников компании в вопросах информационной безопасности	2 дня	2400 за 2 часа	Учебный центр Информзащита	Программа обучения; Семинар; Тренинг; Курсы
Разработка политик информационной безопасности и программ повышения компетенции персонала	2 дня	28000	Учебный Центр «Микроинформ»	Электронный курс + политика по информационной безопасности
Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных	9 дней	44187	Softline	Очная форма обучения, с применением дистанционных методов

Заключение

Специалист, формирующий цифровой контент, с одной стороны, должен обладать профессиональными компетенциями в сфере информационно-коммуникационных технологий, программно-технического обеспечения, а с другой стороны иметь качественную подготовку в исследуемой области, знать особенности предметной области, владеть профессиональными компетенциями в сфере семантической обработки информации.

В ходе данной дипломной работы был разработан Web-сайт, Вики-страница, ментальная карта и HTML-справка для сотрудников финансового предприятия, которые готовы к применению.

Созданный цифровой контент, удовлетворяет всем требованиям, поставленным на этапе постановки задачи, а также ориентирован на изучение основ по информационной безопасности для сотрудников финансовых предприятий. Подобраны современные методы и средства практической реализации, полученные результаты предоставлены в рациональной форме.

В процессе разработки были обоснованы потребности в Web-сайте и другом представленном цифровом контенте. Можно с уверенностью сказать, что цифровой контент справляется с одной из главных задач - повышение осведомленности об актуальных угрозах, мерах и способах реализации атак и средствах защиты, фокусировка внимания сотрудников на важности обеспечения этих проблем и т.п.

Созданный цифровой контент обеспечивает необходимые условия для предотвращения информационных угроз, оптимизация затрат на информационную безопасность, сокращение репутационных рисков компании, а также повышения экономической эффективности деятельности предприятия.

И наконец, была рассчитана экономическая стоимость проекта.

Список литературы

1) Абросимова, М.А. Информационные технологии в государственном и муниципальном управлении: Учебное пособие / М.А. Абросимова. - М.: КноРус, 2013. - 248 с.
2) Акперов, И.Г. Информационные технологии в менеджменте: Учебник / И.Г. Акперов, А.В. Сметанин, И.А. Коноплева. - М.: НИЦ ИНФРА-М, 2013. - 400 с.
3) Алешин, Л.И. Информационные технологии: Учебное пособие / Л.И. Алешин. - М.: Маркет ДС, 2011. - 384 с.
4) Алиев, В.С. Информационные технологии и системы финансового менеджмента: Учебное пособие / В.С. оглы Алиев. - М.: Форум, ИНФРА-М, 2011. - 320 с.
5) Анисимова Т.И. Дистанционное обучение как одна из интерактивных форм подготовки специалистов в вузе / Т.И. Анисимова, Л.А. Краснова // Сборник научных трудов Sworld по материалам международной научно-практической конференции. - 2013. - Т. 16, № 1. - С. 78-81.
6) Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
7) Бубнова Н. Г. Информатика в экономике: учебное пособие / Н. Г. Бубнова и др. – Москва: Вузовский учебник, 2010. – 476 с.
8) Вдовин, В.М. Информационные технологии в финансово-банковской сфере: Практикум / В.М. Вдовин. - М.: Дашков и К, 2012. - 248 с.
9) Венделева, М.А. Информационные технологии в управлении: Учебное пособие для бакалавров / М.А. Венделева, Ю.В. Вертакова. - М.: Юрайт, 2013. - 462 с.
10) Гаврилов, Л.П. Информационные технологии в коммерции: Учебное пособие / Л.П. Гаврилов. - М.: НИЦ ИНФРА-М, 2013. - 238 с.
11) Гагарина Л.Г., Кокорева Е.В., Виснадул Б.Д. Технология разработки программного обеспечения: Уч. пособие.- М.: ИД «ФОРУМ»: ИНФРА-М, 2015.- 400с.- (Высшее образование)
12) Гончарик Н. Г. Цифровые мультимедийные технологии – смысловые средства передачи информационного содержания // Проблемы создания информационных технологий : сб. науч. тр. – 2012. – Вып. 21. – С. 74-76.

13) Гохберт, Г.С. Информационные технологии: учебник для студентов учреждений сред. проф. образования / Г.С. Гохберт, А.В. Зафиевский, А.А. Короткин. – 8-е изд., испр. –М.: Академия, 2013. – 208 с. – (Сред.проф. образование)
14) Карп Е. И. Роль интерактивных мультимедийных систем в вопросе информационного обеспечения деятельности управленческих структур // Вестн. акад. права и упр. – 2010. – № 21. – С. 159-165.
15) Коваленко В.В. Проектирование информационных систем: уч. пособие.- М.: ФОРУМ: ИНФРА-М, 2014.- 320с.- (Высшее образование).
16) Коротков Э.М. Корпоративная социальная ответственность: учебник для бакалавров; допущено УМО по образованию в области менеджмента / ред. Э.М. Коротков. - М.: Юрайт, 2013. - 445 с. - (Серия: Бакалавр. Базовый курс)
17) Лукасевича И.Я, Титоренко Г.А. Информационные ресурсы и технологии в финансовом менеджменте: Учебник / Под ред. И.Я. Лукасевича, Г.А. Титоренко. - М.: ЮНИТИ-ДАНА, 2012
18) Максимов, Н.В. Современные информационные технологии: Учебное пособие / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - М.: Форум, 2013. - 512 с.
19) Одинцова Б.Е. и проф. Романова А.Н. Информационные ресурсы и технологии в экономике: Учебное пособие / Под ред. проф. Б.Е. Одинцова и проф. А.Н. Романова. - М.: Вузовский учебник: НИЦ Инфра-М, 2013 ЭБС Знаниум
20) Олейник, П.П. Корпоративные информационные системы: учебник для вузов. Стандарт третьего поколения / П.П.Олейник. – СПб: Питер, 2012. – 176 с.: ил.
21) Орлов С.М. Внутренний аудит в современной системе корпоративного управления компанией: Практическое пособие / С.Н. Орлов. - М.: НИЦ ИНФРА-М, 2015 ЭБС Знаниум
22) Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.

23) Полякова В.П. Информатика для экономистов: учебник для академического бакалавриата/Под ред. В.П. Полякова.- М.: Юрайт, 2015.- 524с.- Серия: Бакалавр. Академический курс.
24) Рыхтикова Н.А. Анализ и управление рисками организации: Учебное пособие / Н.А. Рыхтикова. - 2-е изд. - М.: Форум, 2014 ЭБС Знаниум
25) Трофимов В.В. Информационные технологии в экономике и управлении: учебник; рекомендовано МО и науки РФ / ред. В. В. Трофимов. - М.: Юрайт, 2011. - 478 с.
26) Федорова, Г.Н. Информационные системы: Учебник для студ. учреждений сред. проф. образования / Г.Н. Федорова. - М.: ИЦ Академия, 2013. - 208 с.
27) Холин А. Н. Ситуационные центры: перспективы цифровых технологий. Площадка для апробации цифровых технологи // Науч. периодика: проблемы и решения. – 2011. – № 6. – С. 6-9.
28) Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.
29) Ясенев, В.Н. Информационные системы и технологии в экономике.: Учебное пособие для студентов вузов / В.Н. Ясенев. - М.: ЮНИТИ-ДАНА, 2012. - 560 с.
30) Ассоциация по сертификации «Русский Регистр»[Электронный ресурс]. -Режим доступа: http://www.rusregister.ru/ (17.02.2015);
31) Поддержка Office [Электронный ресурс]. -Режим доступа:https://support.office.com/;
32) Программирование «Realcoding.Net» - Программирование линейное, C++, Delphi, C#, .NET, 1C, системы, языки, обучение [Электронный ресурс]. -Режим доступа:http://www.realcoding.net/;
33) Свободная электронная библиотека «wikipedia.org»[Электронный ресурс]. -Режим доступа:https://ru.wikipedia.org/;
34) Компания «Лаборатория Касперского» [Электронный ресурс]. -Режим доступа:http://media.kaspersky.com/;
35) «Хабрахабр» (или «Хабр») — крупнейший в Европе ресурс для IT-специалистов [Электронный ресурс]. -Режим доступа:http://habrahabr.ru/company/pt/blog/239379/;

36) «Dehack.ru» проект, являющийся информационным ресурсом, представляющим и раскрывающим проблематику защиты конфиденциальной информации [Электронный ресурс]. -Режим доступа:http://dehack.ru/otvetstvennost/;
37) Экономика информационной безопасности: Учебное пособие. – СПб.: НИУИТМО, 2012. – 120 с [Электронный ресурс]. -Режим доступа:http://books.ifmo.ru/file/pdf/923.pdf;
38) «CNews» интернет-портал - ориентированный на полное, оперативное и беспристрастное освещение информационной картины дня рынка высоких технологий [Электронный ресурс]. -Режим доступа:http://www.cnews.ru/news/;
39) Электронное периодическое издание «ИКС-медиа» [Электронный ресурс]. -Режим доступа:http://www.iksmedia.ru/;
40) Средство массовой информации - издательство «Открытые системы» [Электронный ресурс]. -Режим доступа:http://www.osp.ru/;
41) «Мегамозг» — крупнейший в Европе ресурс для IT-специалистов [Электронный ресурс]. -Режим доступа:http://megamozg.ru/;
42) Студопедия.Орг- это информационный сайт для студентов, учащихся в вузах[Электронный ресурс]. -Режим доступа:http://studopedia.org/13-62019.html;
43) Копания «ИТ Идеи 74» - аутсорсинговая компания в области информационных технологий [Электронный ресурс]. -Режим доступа:http://it-ideas74.ru/;
44) «Безопасник» - информационный сайт, освещающий современные системы безопасности[Электронный ресурс]. -Режим доступа:http://bezopasnik.org/;
45) Элькина Е. Повышение квалификации пользователей в области информационной безопасности на основе E-Learning технологий[Электронный ресурс]. -Режим доступа:http://dsec.ru/ipm-research-center/article/raising_the_qualification_of_users_in_the_field_of_information_security/;
46) Журнал «IT-спец»[Электронный ресурс]. -Режим доступа:http://www.itspecial.ru/;

47) Журнал «BIS Journal − Информационная безопасность банков» [Электронный ресурс]. -Режим доступа:http://www.journal.ib-bank.ru/;
48) Национальный форум информационной безопасности «Инфофорум» [Электронный ресурс]. -Режим доступа:http://infoforum.ru/;
49) Журнал «Вестник УрФО. Безопасность в информационной сфере» [Электронный ресурс]. -Режим доступа:http://www.info-secur.ru/
50) Российский комитет программы ЮНЕСКО «Информация для всех» [Электронный ресурс]. -Режим доступа:http://ifapcom.ru/